Modular curves and cyclotomic fields[1]

Romyar T. Sharifi

[1]This is a draft from March 12, 2018. Please check back regularly for the latest version.

Contents

Chapter 1. Introduction 5

Chapter 2. Arithmetic of cyclotomic fields 9
2.1. Class numbers and L-functions 9
2.2. The Herbrand-Ribet Theorem 13
2.3. Iwasawa modules 15
2.4. Kubota-Leopoldt p-adic L-functions 20
2.5. The Iwasawa main conjecture 21

Chapter 3. Theory of modular forms 25
3.1. Modular curves over $\mathbb{C}$ 25
3.2. Moduli-theoretic interpretation 27
3.3. Modular forms 29
3.4. Homology and cohomology 34
3.5. Galois representations 38

Chapter 4. Hida theory and the main conjecture 41
4.1. Ordinary forms 41
4.2. Hida theory 42
4.3. Proof of the main conjecture 47
4.4. The map Υ 49

Chapter 5. Modular symbols and arithmetic 53
5.1. Galois cohomology and cup products 53
5.2. Iwasawa cohomology 58
5.3. K-groups and Steinberg symbols 60
5.4. The map ϖ 61
5.5. A conjecture and known results 66

Appendix A. Project descriptions 71
A.1. First project 71
A.2. Second project 72
A.3. Third project 73
A.4. Fourth project 74

Bibliography 75

CHAPTER 1

Introduction

These notes concern the arithmetic of the p^nth cyclotomic fields $F_n = \mathbb{Q}(\mu_{p^n})$ for an odd prime p and a positive integer n. Here, μ_{p^n} denotes the group of p^nth roots of unity inside the complex numbers. When we speak of arithmetic, we speak not just of field elements but of algebraic integers in this field, which is to say elements of the ring $\mathcal{O}_n = \mathbb{Z}[\mu_{p^n}]$ generated by the p^nth roots of unity. This ring is of course also generated by the single primitive p^nth root of unity $\zeta_{p^n} = e^{2\pi i/p^n}$.

The failure of the rings $\mathcal{O}_n$ to always be principal ideal domains is measured by the class group Cl_n of F_n. Of particular interest is its Sylow p-subgroup A_n, which consists of the elements of p-power order. The prime p is said to be regular if $A_n = 0$ and irregular otherwise. In 1850, Kummer showed that Fermat's last theorem holds for regular prime exponents, employing the factorization

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$$

in $\mathbb{Z}[\mu_p]$ for integers x and y.

Iwasawa studied the growth of the groups A_n as n increases. In particular, he showed that their orders have a surprising regularity. That is, there exist nonnegative integers μ and λ and an integer ν such that

$$|A_n| = p^{p^n\mu+n\lambda+\nu}$$

for all sufficiently large n [**Iwa1**]. Each of these groups A_n has an action of the Galois group $\mathrm{Gal}(F_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$, and in particular of the group $\Gamma_n = \mathrm{Gal}(F_n/F_1)$, which is noncanonically isomorphic to $\mathbb{Z}/p^{n-1}\mathbb{Z}$. The inverse limit $X_\infty = \varprojlim_n A_n$ of the groups A_n under norm maps is a profinite group with the corresponding profinite topology. By definition, it has a continuous action of the group $\Gamma = \mathrm{Gal}(F_\infty/F_1)$, where $F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_n F_n$. The group Γ is then noncanonically isomorphic to $\mathbb{Z}_p$, and by continuity, the action extends to an action of the completed group ring $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \cong \varprojlim_n \mathbb{Z}_p[\Gamma_n]$ on X_∞. This group ring is in turn continuously isomorphic to the one variable power-series ring $\mathbb{Z}_p[\![T]\!]$, with the isomorphism determined by a choice of topological generator γ of Γ. That is, $\gamma - 1$ is sent to T, and this allows us to identify the two compact $\mathbb{Z}_p$-algebras.

As a module over this group ring, X_∞ can be seen to be finitely generated and torsion over Λ. Moreover, its coinvariant group $(X_\infty)_{\mathrm{Gal}(F_\infty/F_n)}$, which is the maximal quotient of X_∞ on which the action of Γ factors through Γ_n, is isomorphic to A_n via the canonical map given by definition of the inverse limit. The statement on the order of A_n then reduces to a statement about finitely generated, torsion modules over Λ, as was observed by Serre [**Ser**]. That is, any

finitely generated torsion Λ-module M is "pseudo-isomorphic" to a direct sum of quotients of Λ by principal ideals, in the sense that there exists a Λ-module homomorphism to such a direct sum with finite kernel and cokernel. The product of the latter principal ideals is an invariant of M called the characteristic ideal of M.

Now, the group ring $\mathbb{Z}_p[\Delta]$ of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ also acts on X_∞, and X_∞ breaks into a direct sum of components

$$X_\infty^{(i)} = \{x \in X_\infty \mid \delta(x) = a^i x\},$$

where δ is a generator of Δ and $a \in \mathbb{Z}_p^\times$ is the unique $(p-1)$th root of unity such that $\delta(\zeta_p) = \zeta_p^a$. The main conjecture of Iwasawa theory (cf. [**Iwa4, Iwa5**]) states that the characteristic ideal of $X_\infty^{(i)}$ for an odd integer i has characteristic ideal generated by a power series g_i attached to a Kubota-Leopoldt p-adic L-function $L_p(\omega^{1-i}, s)$ in the sense that $g_i(\upsilon^s - 1) = L_p(\omega^{1-i}, s)$ for all $s \in \mathbb{Z}_p$ for the topological generator υ of $1 + p\mathbb{Z}_p$ that is the evaluation of the p-adic cyclotomic character on γ.

The main conjecture was proven by Mazur and Wiles in 1984 using the geometry of modular curves [**MaWi1**]. In fact, what they proved is that for each odd i, the characteristic ideal of $X_\infty^{(i)}$ is divisible by (g_i). This is sufficient as the analytic class number formula tells us that the product of the (g_i) is the product of the characteristic ideals of $X_\infty^{(i)}$. Mazur and Wiles construct a large enough unramified abelian pro-p extension of F_∞ with the desired action of Δ, significantly extending a method introduced by Ribet [**Rib**]. They do so by studying the irreducible two-dimensional Galois representations attached to cuspidal eigenforms that satisfy congruences with Eisenstein series modulo primes over p. By virtue of these congruences, these representations are residually reducible: in fact, there exists a Galois-stable lattice in the representation such that its reduction modulo the prime is unramified upon restriction to the absolute Galois group of F_∞. To find a large enough unramified extension to produce $X_\infty^{(i)}$ via the isomorphism of class field theory, they must consider cusp forms of increasing p-power level.

The cusp forms used in the main conjecture can be placed in a family of cusp forms of varying level and weight, and if one likes, may be viewed as a single modular form with coefficients in a finite flat algebra over Λ, with the variable coming from certain diamond operators. The Galois representations may be similarly encapsulated in a single two-dimensional representation over the Hecke algebra acting on such Λ-adic modular forms. This is made possible by the fact that the modular forms under consideration are ordinary: their pth Fourier coefficients are units, and the good control one has over the growth of spaces of such forms is the subject of Hida theory, which has much of the flavor of Iwasawa theory.

The Mazur-Wiles proof of the main conjecture indicates that the geometry of modular curves "near the cusps" has much to say about the arithmetic of cyclotomic fields. That is, the "Eisenstein ideal" determining the congruences between our Λ-adic cusp forms and Eisenstein series is essentially the annihilator of the cusp at ∞. So, when we look at residual representations attached to our cusp forms, we are essentially exploring the geometry of a modular curve near ∞.

The characteristic ideal of an Iwasawa module being a rather rough invariant of its structure, one might ask how far one can push this connection between geometry and arithmetic. The construction of the unramified extension in the Mazur-Wiles proof is rather far from canonical,

but this can be improved. Out of the residual Galois representation attached to the Λ-adic cusp forms one uses in the proof, one can construct a canonical map Υ from the Tate twist $X_\infty^{(i)}(1)$ to a space of Λ-adic cusp forms $\mathfrak{S}$ reduced modulo an Eisentein ideal I_i. This map is not obviously an isomorphism, but that it is has recently been shown by M. Ohta [**Oht4**].

There is also a map $\varpi\colon \mathfrak{S}/I_i\mathfrak{S} \to X_\infty^{(i)}(1)$ in the opposite direction that is explicitly defined to take certain compatible sequences of classes in the real parts of homology groups of modular curves to compatible sequences of cup products of cyclotomic units in Galois cohomology. As we shall explain, the two maps Υ and ϖ are conjecturally inverse to each other. A major result in this direction, in which the derivative $L_p(\omega^{1-i}, s)$ intervenes (and which, though weaker, may be the most natural statement), has been proven by Fukaya and Kato [**FuKa**].

ACKNOWLEDGMENTS. The author thanks Preston Wake and Ashay Burungale for detailed comments on these notes that have improved them significantly.

CHAPTER 2

Arithmetic of cyclotomic fields

We shall not attempt to describe results in their most general form in these notes. For a more complete accounting, we suggest the book of Washington [**Was**] or our lecture notes [**Sha5**] (still in draft form at this writing). We will frequently restrict our discussion to the p-power cyclotomic fields.

2.1. Class numbers and L-functions

We recall the definition of the Dedekind zeta function of a number field.

DEFINITION 2.1.1. The Dedekind zeta function of a number field F is the meromorphic continuation to $\mathbb{C}$ of the series

$$\zeta_F(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_F} (N\mathfrak{a})^{-s},$$

which converges on $s \in \mathbb{C}$ satisfying $\mathrm{Re}(s) > 1$. Here, the sum is taken over ideals $\mathfrak{a}$ of the ring of integers $\mathcal{O}_F$ of F, and $N\mathfrak{a} = [\mathcal{O}_F : \mathfrak{a}]$ is the absolute norm of $\mathfrak{a}$.

Also associated to F is a positive real number known as its regulator R_F, formed out of the determinant of a matrix with entries given by the logarithms of all but one of the real and complex absolute values on F applied to a set of generators of the units group $\mathcal{O}_F^\times$, modulo torsion. This regulator appears in proofs of Dirichlet's unit theorem.

THEOREM 2.1.2 (ANALYTIC CLASS NUMBER FORMULA). *Let F be a number field. Then*

$$\lim_{s \to 1} (s-1)\zeta_F(s) = \frac{2^{r_1(F)}(2\pi)^{r_2(F)} h_F R_F}{w_F |d_F|^{1/2}},$$

where for F, the quantities $r_1(F)$ and $r_2(F)$ are respectively the number of its real and complex places, h_F is its class number, R_F is its regulator, w_F is the number of roots of unity it contains, and d_F is its discriminant.

DEFINITION 2.1.3. For a commutative ring R (with 1), an R-valued Dirichlet character is a multiplicative function $\chi \colon \mathbb{Z}/N\mathbb{Z} \to R$ for some positive integer N known as its modulus, that is defined as 0 on all non-units in $\mathbb{Z}/N\mathbb{Z}$. By composition with reduction modulo N, we typically view χ as a function on $\mathbb{Z}$.

REMARK 2.1.4. When R is not specified, we take it either to be $\mathbb{C}$ or an arbitrary ring, as needed in the context.

DEFINITION 2.1.5. The minimal positive integer such that the restriction of a Dirichlet character χ to $(\mathbb{Z}/N\mathbb{Z})^\times$ of modulus N factors through $(\mathbb{Z}/f\mathbb{Z})^\times$ is known as its conductor. We say that χ is primitive if its modulus and conductor agree.

DEFINITION 2.1.6. We say that a Dirichlet character χ is odd if $\chi(-1) = -1$, and even if $\chi(-1) = 1$.

DEFINITION 2.1.7. Let χ be a Dirichlet character of modulus N. The Dirichlet L-function associated to a Dirichlet character χ is the meromorphic continuation to $\mathbb{C}$ of the series

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

which converges on $s \in \mathbb{C}$ satisfying $\mathrm{Re}(s) > 1$.

REMARK 2.1.8. The L-function $L(\chi, s)$ is entire unless χ is the trivial character of its modulus.

REMARK 2.1.9. The L-series $L(\chi, s)$ has an Euler product expansion

$$L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}.$$

By the Kronecker-Weber theorem, any abelian number field F (i.e., number field that is an abelian extension of $\mathbb{Q}$) is contained in $\mathbb{Q}(\mu_N)$ for some $N \geq 1$, in which case $\mathrm{Gal}(F/\mathbb{Q})$ is identified with a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times$ via the Nth cyclotomic character. Let $X(F)$ denote the set of primitive Dirichlet characters of conductor dividing N that, viewed as characters on $(\mathbb{Z}/N\mathbb{Z})^\times$, factor through $\mathrm{Gal}(F/\mathbb{Q})$ under this identification.

PROPOSITION 2.1.10. *For an abelian number field F, we have*

$$\zeta_F(s) = \prod_{\chi \in X(F)} L(\chi, s).$$

EXERCISE 2.1.11. Prove Proposition 2.1.10 by examining the Euler product expansions of the two sides.

We next turn to the special values of our Dirichlet L-functions and the Riemann zeta function. For these, we introduce the Bernoulli numbers and their generalized counterparts.

DEFINITION 2.1.12. The nth Bernoulli number B_n is the value of the nth derivative of $\frac{x}{e^x - 1}$ at 0.

The Bernoulli numbers B_n for odd n are 0 except for $B_1 = -\frac{1}{2}$, and the Bernoulli numbers for even n starting with B_0 are

$$1, \frac{1}{6}, -\frac{1}{30}, \frac{1}{42}, -\frac{1}{30}, \frac{5}{66}, -\frac{691}{2730}, \frac{7}{6}, \frac{3617}{510} \ldots.$$

These numbers are nearly the special values of the Riemann zeta function at nonpositive integers. That is, we have the following.

REMARK 2.1.13. The Bernoulli numbers satisfy

$$\zeta(1 - n) = (-1)^{n-1} \frac{B_n}{n}$$

for $n \geq 1$.

Let us list the prime factorizations of the absolute values of the numerators of the $\frac{B_k}{k}$ for even $k \geq 2$:

$$1, 1, 1, 1, 1, 691, 1, 3617, 43867, 283 \cdot 617, 131 \cdot 593, ...$$

The prime numbers which occur in this list are known as irregular primes. They play a central role in our study.

We also have a generalized notion of Bernoulli numbers for Dirichlet characters.

DEFINITION 2.1.14. The nth generalized Bernoulli number $B_{n,\chi}$ for a Dirichlet character χ of modulus N is the nth derivative at 0 of the polynomial

$$\sum_{a=1}^{N} \chi(a) \frac{xe^{ax}}{e^{Nx} - 1}.$$

EXAMPLE 2.1.15. For any Dirichlet character χ of modulus dividing N, we have

$$B_{1,\chi} = \frac{1}{N} \sum_{a=1}^{N} \chi(a) a.$$

REMARK 2.1.16. Similarly to the values of Riemann zeta function, we have

$$L(\chi, 1 - n) = -\frac{B_{n,\chi}}{n}$$

for all $n \geq 1$.

DEFINITION 2.1.17. A number field is totally real if its archimedean places are all real, and it is CM if it is a purely imaginary (i.e., having only complex archimedean places) quadratic extension of a totally real field.

Any abelian number field F is either totally real or CM. Let F^+ denote the maximal totally real subfield of F, which is of index at most 2 in F.

DEFINITION 2.1.18. The plus and minus parts of the class number of a CM number field F are the integers

$$h_F^+ = h_{F^+} \quad \text{and} \quad h_F^- = \frac{h_F}{h_F^+}.$$

EXERCISE 2.1.19. Show that h_F^- is an integer.

The analytic class number formula yields individual formulas for the plus and minus parts of the class number. We write $a \sim b$ for integers a and b if they agree up to a power of 2. Let $X^-(F)$ denote the set of primitive odd Dirichlet characters in $X(F)$.

THEOREM 2.1.20. *For any positive integer N, we have*

$$h^-_{\mathbb{Q}(\mu_N)} \sim N \prod_{\chi \in X^-(\mathbb{Q}(\mu_N))} B_{1,\chi}.$$

The ring of integers of $\mathbb{Q}(\mu_N)$ is $\mathbb{Z}[\mu_N]$, and we let $E_N = \mathbb{Z}[\mu_N]^\times$ denote its unit group for brevity. By Dirichlet's unit theorem, the rank of E_N is $\frac{\varphi(N)}{2} - 1$. Let us fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, which singles out the primitive Nth root of unity $\zeta_N = e^{2\pi i/N}$.

REMARK 2.1.21. The element $1-\zeta_N \in \mathbb{Q}(\mu_N)^\times$ is a unit if N is composite, but it is merely a p-unit (i.e., a unit in $\mathbb{Z}[\frac{1}{p}, \mu_N]$) if N is a power of p.

DEFINITION 2.1.22. For $N \geq 1$, the group of cyclotomic units C_N in $\mathbb{Q}(\mu_N)$ is the intersection with E_N of the subgroup of $\mathbb{Q}(\mu_N)^\times$ generated by its roots of unity and the elements $1-\zeta_N^i$ with $1 \leq i < N$.

THEOREM 2.1.23. *For any positive integer N, the group C_N is of finite index in E_N. We have*

$$h^+_{\mathbb{Q}(\mu_N)} \sim [E_N : C_N],$$

and this is an equality if N is a prime power.

Let us now specialize back to our fields of interest, the fields $F_n = \mathbb{Q}(\mu_{p^n})$ for a prime p, which for now we shall not require to be odd. The Galois group $\mathrm{Gal}(F_n/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$ via the modulo p^n cyclotomic character that is determined by the power to which an element raises ζ_{p^n}. As such, it breaks up as a product $\Delta \times \Gamma_n$, where if p is odd, $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and Γ_n is a cyclic p-group. If $p = 2$, we take Δ to be the order 2 subgroup generated by complex conjugation and Γ_n to be the cyclic 2-group generated by elements which are 1 modulo 4. We let

$$q = \begin{cases} p & \text{if } p \text{ is odd} \\ 4 & \text{if } p = 2, \end{cases}$$

and we set $F = \mathbb{Q}(\mu_q)$.

DEFINITION 2.1.24. Let ω denote the homomorphism $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ that is the composition

$$\mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/q\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times$$

of reduction modulo q and the unique homomorphism splitting it. We also denote by ω the Dirichlet character of modulus q induced by the latter injection.

PROPOSITION 2.1.25. *We have*

$$B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \bmod p\mathbb{Z}_p$$

for any positive integer $k \geq 2$ with $k \not\equiv 0 \bmod p-1$.

As $B_{1,\omega^{-1}}$ has p-adic valuation -1, Theorem 2.1.20 has the following corollary.

COROLLARY 2.1.26. *The class number h_F^- is divisible by p if and only if p divides B_k for some positive even integer $k < p-1$.*

DEFINITION 2.1.27. We say that a prime p is regular if $p \nmid h_F$. Otherwise p is said to be irregular.

By a result of Kummer, p is regular if and only if $p \nmid h_F^-$. Thus, p is regular if and only if p divides the numerator of some B_k for a positive even $k < p-1$.

It is known that there are infinitely many irregular primes, and though heuristically speaking there are more regular primes than irregular primes less than any given bound, it is still an open question as to whether there are infinitely many regular primes.

EXAMPLE 2.1.28. The smallest irregular primes are 37, 59, 67, 101, and 103. For instance, $37 \mid B_{32}$, $59 \mid B_{44}$, and $67 \mid B_{58}$.

DEFINITION 2.1.29. The index of irregularity of a prime is the number of positive even $k < p-1$ such that $p \mid B_k$.

EXAMPLE 2.1.30. The smallest prime having index of irregularity greater than one is 157, which divides B_{62} and B_{110}. The prime 691 divides B_{12} and B_{200}.

Kummer made the following conjecture regarding h_F^+ in 1849 in a letter to Kronecker, and it was later rediscovered by Vandiver around 1920, after whom it is typically named. It has been verified for primes $p < 39 \cdot 2^{22} = 163557355$ by Buhler and Harvey [**BuHa**].

CONJECTURE 2.1.31 (KUMMER-VANDIVER CONJECTURE). *The p-part of the class number of F^+ is* 1.

Since it provides an interesting example, we remark that Weber conjectured the following for $p = 2$ in 1886, and Coates has asked whether its generalization to odd p holds.

CONJECTURE 2.1.32. *For any prime p, let $\mathbb{Q}_n$ denote the maximal (cyclic) p-extension of $\mathbb{Q}$ in F_n. Then $h_{\mathbb{Q}_n} = 1$.*

2.2. The Herbrand-Ribet Theorem

Now let us suppose that p is odd. Let A denote the p-part of the class group of $F = \mathbb{Q}(\mu_p)$. Let $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, which we identify with $(\mathbb{Z}/p\mathbb{Z})^\times$. We let ω also denote the unique character $\Delta \to \mathbb{Z}_p^\times$ with reduction modulo p equal to the mod p cyclotomic character.

The group A has an action of Δ, so being that A is a p-group, it has the structure of a $\mathbb{Z}_p[\Delta]$-module. Like all $\mathbb{Z}_p[\Delta]$-modules, the group A has a canonical decomposition as a direct sum

$$A = \bigoplus_{i=0}^{p-2} A^{(i)},$$

where

$$A^{(i)} = \{a \in A \mid \delta(a) = \omega(\delta)^i a \text{ for all } \delta \in \Delta\}.$$

Note that $A^{(i)} = A^{(j)}$ if $i \equiv j \bmod p-1$.

The following theorem of Leopoldt [**Leo**] is known as Leopoldt's reflection theorem (or "Spiegelungsatz").

THEOREM 2.2.1 (LEOPOLDT). *For even k, we have*

$$\dim_{\mathbb{F}_p}(A/pA)^{(k)} \leq \dim_{\mathbb{F}_p}(A/pA)^{(1-k)} \leq \dim_{\mathbb{F}_p}(A/pA)^{(k)} + 1.$$

EXERCISE 2.2.2. Prove this using Kummer theory (see the method of the proof of Theorem 2.3.18 below).

In particular, this theorem implies that if $A^{(1-k)} = 0$, then $A^{(k)} = 0$. If Vandiver's conjecture holds so that $A^{(k)} = 0$, the theorem tells us that $A^{(1-k)}$ is cyclic. In 1932, Herbrand proved that if $A^{(1-k)} \neq 0$, then $p \mid B_k$ [**Her**]. The converse was proven by Ribet in 1976 [**Rib**].

THEOREM 2.2.3 (HERBRAND-RIBET). *Let p be an odd prime, and let k be even with $2 \leq k \leq p-3$. We have $A^{(1-k)} \neq 0$ if and only if $p \mid B_k$.*

We explain how Herbrand's theorem follows from a result of Stickelberger's.

SKETCH OF PROOF OF HERBRAND'S THEOREM. The Stickelberger element of $\mathbb{Q}_p[\Delta]$ is

$$\theta = \frac{1}{p}\sum_{a=1}^{p-1} a[a]^{-1},$$

and the Stickelberger ideal of $\mathbb{Z}_p[\Delta]$ is the intersection $\mathcal{I} = \mathbb{Z}_p[\Delta]\theta \cap \mathbb{Z}_p[\Delta]$. Stickelberger proved that $\mathcal{I}$ annihilates A. Moreover, it is easy to see that $([b]-b)\theta \in \mathcal{I}$ for all $b \in \mathbb{Z}$ prime to p, where $[b]$ denotes the group element of b. The action of this element on $x \in A^{(1-k)}$ is given by

$$([b]-b)\theta x = (\omega^{1-k}(b)-b)B_{1,\omega^{k-1}}x,$$

but it is also zero. Since $k \not\equiv 0 \bmod p$, the element $\omega^{1-k}(b) - b$ is a unit for some b, and therefore $B_{1,\omega^{k-1}}$ annihilates x. In particular, if $A^{(1-k)} \neq 0$, then $B_{1,\omega^{k-1}} \notin \mathbb{Z}_p^\times$. By the Kummer congruence of Proposition 2.1.25, we have the result. □

We sketch a proof of the opposite implication which uses the theory of modular forms, and in particular congruences between cusp forms and Eisenstein series. We use this sketch as motivation for these concepts, which we elaborate upon in the following chapter. The reader may wish to return to this proof anew after reviewing those concepts. Our sketch is in the spirit of Ribet's proof, but what we write is more along the lines of the approach of Kurihara [**Kur**] and Harder-Pink [**HaPi**]. For an algebraic extension K of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$, let us use $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ to denote its absolute Galois group.

SKETCH OF PROOF OF RIBET'S THEOREM. Suppose that p divides B_k. Consider the weight k, level 1 Eisenstein series

$$E_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sum_{d|n} d^{k-1}q^n. \tag{2.2.1}$$

Modulo p, the Eisenstein series E_k has trivial constant term and so is a cusp form, being that ∞ is the only cusp of $\mathrm{SL}_2(\mathbb{Z})$. This cusp form lifts to a weight k newform $f = \sum_{n=1}^{\infty} a_n q^n$ on $\mathrm{SL}_2(\mathbb{Z})$. Attached to this f is an irreducible 2-dimensional Galois representation $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ that is unramified outside of p and characterized by the properties that $\det(\rho_f(\varphi_\ell)) = \ell^{k-1}$ and $\mathrm{Tr}(\rho_f(\varphi_\ell)) = a_\ell$ for any Frobenius φ_ℓ at ℓ for all primes $\ell \neq p$. In fact, this representation takes values in the $\mathrm{GL}_2(K_f)$, where K_f is the field of coefficients of f over $\mathbb{Q}_p$. Let V_f denote the corresponding 2-dimensional vector space over K_f.

For us, it is easiest to twist V_f by the $(1-k)$th power of the cyclotomic character: i.e., we consider $V_f' = V_f(1-k)$ and the resulting representation $\rho_f' \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ with determinant χ_p^{1-k} for the p-adic cyclotomic character $\chi_p \colon G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$. There exists a basis of V_f' such that the restriction of ρ_f' to a decomposition group D_p at a given prime over p is lower-triangular, and invariant group of $(V_f')^{I_p}$ of the inertia subgroup I_p is 1-dimensional.

In order to consider a residual representation associated to ρ_f, we must first choose a Galois stable lattice L_f in V_f', which is to say a free module of rank 2 over the valuation ring $\mathcal{O}_f$ of K_f. In fact, V_f' is itself constructed out of a canonical such lattice H_f, for instance as a certain subquotient group of a first étale cohomology group of a modular curve. Let π_f denote a uniformizer of $\mathcal{O}_f$, and let $\mathbb{F}_f = \mathcal{O}_f/\pi_f\mathcal{O}_f$ be the residue field. If f were not congruent to an Eisenstein series, then the residual representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_f}(H_f/\pi_f H_f)$ would be irreducible, and every Galois stable lattice in V_f' would have an isomorphic residual representation. However, in our case, every residual representation is reducible, and different choices of lattices can yield non-isomorphic residual representations.

The irreduciblity of ρ_f precludes the residual representations attached to Galois-stable lattices in V_f from all being semisimple, i.e., direct sums of two 1-dimensional representations. There exist smallest and largest non-split Galois-stable lattices with I_p-invariant group equal to $(H_f)^{I_p}$. The smallest such, which is our L_f, has $H_f^{I_p}/\pi_f H_f^{I_p}$ as a global quotient, hence is $G_{\mathbb{Q}_p}$-split. One can show that this quotient has trivial $G_{\mathbb{Q}}$-action, noting that $a_p(f) \equiv a_p(E_k) \equiv 1 \bmod \pi_f$ to get the triviality of the action of a Frobenius at p. Thus, $\bar{\rho}_f' \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_f}(L_f/\pi_f L_f)$ is a nontrivial unramified homomorphism upon restriction to the kernel of ω^{1-k}. In particular, $\bar{\rho}_f'$ has the form

$$\begin{pmatrix} \omega^{1-k} & * \\ 0 & 1 \end{pmatrix}$$

for a good choice of basis, where $*$ is a 1-cocycle that restricts to an unramified character on $G_{\mathbb{Q}(\mu_p)}$. The image of this homomorphism is a nontrivial quotient of A by class field theory, and the action of Δ on this quotient through lifting and conjugating is given by ω^{1-k}, as required. □

2.3. Iwasawa modules

We continue to let p be an odd prime. Let A_n denote the p-part of the class group of F_n, which is a module over $\mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$. For $n \geq m$, we may consider the maps $A_m \to A_n$ and $A_n \to A_m$ induced by the inclusion of ideal groups and the norm map on ideals, respectively. These maps respect the $\mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$-actions on both groups, viewing $(\mathbb{Z}/p^m\mathbb{Z})^\times$ as a quotient of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. We let

$$A_\infty = \varinjlim_n A_n \quad \text{and} \quad X_\infty = \varprojlim_n A_n,$$

with the direct and inverse limits taken with respect to these maps.

Endowing A_∞ with the discrete topology and X_∞ with the profinite topology, these groups become continuous modules over the completed group ring

$$\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] = \varprojlim_n \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times],$$

which is endowed with the (profinite) topology of the inverse limit. Here, the action is the Galois action through the group $\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$, where $F_\infty = \mathbb{Q}(\mu_{p^\infty})$, the isomorphism being given by the p-adic cyclotomic character $\chi_p \colon G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, defined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_p(\sigma)}$ for $\sigma \in G_{\mathbb{Q}}$ and all $n \geq 1$.

The group $\Gamma = 1 + p\mathbb{Z}_p$ is procyclic, generated for instance by $1 + p$. We fix what may seem a rather unusual choice of generator for later purposes: let $\upsilon \in \Gamma$ be such that

$$(1 - p^{-1}) \log \upsilon = 1, \tag{2.3.1}$$

where $\log\colon 1 + p\mathbb{Z}_p \to \mathbb{Z}_p$ is the p-adic logarithm defined by the Taylor series expansion about 1 of the natural logarithm. The profinite $\mathbb{Z}_p$-algebra $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ is isomorphic to the completed group ring $\mathbb{Z}_p[\![T]\!]$ through such a choice of υ. Explicitly, we have

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![\Gamma]\!]$$

via the unique continuous $\mathbb{Z}_p$-linear isomorphism taking T to $\gamma - 1$, where $\gamma = [\upsilon]$ is the group element of υ.

Remark 2.3.1. In fact, there is no reason we cannot work in greater generality. That is, for any prime p and $n \geq 1$ or $n = \infty$, let $\mathbb{Q}_n$ denote the fixed field of $\Delta = (\mathbb{Z}/q\mathbb{Z})^\times$ in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Fixing a number field F, we can then set $F_n = F\mathbb{Q}_n$. We then have $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, and F_∞ is called the cyclotomic $\mathbb{Z}_p$-extension of F. Defining A_n as the p-part of the class group of F_n, we can define A_∞ and X_∞ as before. These are then modules over $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$, for $\Gamma = \mathrm{Gal}(F_\infty/F)$, which is again procyclic.

The group X_∞ is a finitely generated, torsion Λ-module. This follows by Nakayama's lemma from the fact that (at least for $F = \mathbb{Q}(\mu_p)$) its Γ-coinvariant group is isomorphic to the finite $\mathbb{Z}_p$-module A_1. The Pontryagin dual group $A_\infty^\vee = \mathrm{Hom}_{\mathrm{cts}}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is also a finitely generated Λ-module, where γ acts on an element f by precomposition with multiplication by γ^{-1}. (In fact, it is a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \Lambda[\Delta]$-module.)

The module theory of finitely generated Λ-modules is particularly nice, as every localization of Λ at a height one prime is a principal ideal domain, for which the structure theory of finitely generated modules is standard. A finitely generated torsion Λ-module M is as a consequence nearly isomorphic to the product of these localizations via the canonical inclusion: the kernel is the maximal finite Λ-submodule of M and the cokernel is finite as well.

Definition 2.3.2. A Λ-module homomorphism with finite kernel and cokernel is called a pseudo-isomorphism. We say that a Λ-module M is pseudo-isomorphic to a Λ-module N if there exists a pseudo-isomorphism $M \to N$ or a pseudo-isomorphism $N \to M$.

For general finitely generated Λ-modules, the existence of a pseudo-isomorphism does not imply the existence of a pseudo-isomorphism in the opposite direction.

Example 2.3.3. The maximal ideal of Λ is (p, T), which injects into Λ with finite cokernel, while there exists no pseudo-isomorphism $\Lambda \to (p, T)$.

For finitely generated-torsion modules, if $M \to N$ is a pseudo-isomorphism, then there does indeed exist a pseudo-isomorphism $N \to M$. That is, if we let $f \in \Lambda$ be an irreducible element outside of the support of M and N, then $M \otimes_\Lambda \Lambda[\frac{1}{f}] \to N \otimes_{\mathbb{Z}_p} \Lambda[\frac{1}{f}]$ is an isomorphism, and if we multiply the inverse by a suitably high power of f, the image of N will lie a finite index submodule of M inside $M \otimes_\Lambda \Lambda[\frac{1}{f}]$.

DEFINITION 2.3.4. A distinguished (or Weierstrass) polynomial in $\mathbb{Z}_p[T]$ is a nonconstant polynomial f satisfying $f \equiv T^{\deg f} \bmod p$

THEOREM 2.3.5 (WEIERSTRASS PREPARATION THEOREM). *Every nonzero element of Λ is the product of a unit, a power of p, and possibly a distinguished polynomial.*

Summarizing what we have said, we obtain the following [**Ser**].

THEOREM 2.3.6 (SERRE). *Every finitely generated Λ-module M is pseudo-isomorphic to a Λ-module of the form*

$$\Lambda^r \oplus \bigoplus_{i=1}^{g} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{h} \Lambda/(p^{\mu_j}), \tag{2.3.2}$$

where $r, g, h \geq 0$, the $f_i \in \Lambda$ are irreducible distinguished polynomials, $k_i \geq 1$ for $1 \leq i \leq g$, and $\mu_j \geq 1$ for $1 \leq j \leq h$. This decomposition is unique up ordering.

The nonnegative integer r in this theorem is the Λ-rank of M, i.e., $r = \dim_{Q(\Lambda)}(M \otimes_\Lambda Q(\Lambda))$, for $Q(\Lambda)$ the quotient field of Λ. Moreover, we may make the following definitions.

DEFINITION 2.3.7. For a finitely generated Λ-module M which is pseudo-isomorphic to a Λ-module as in (2.3.2), the quantities

$$\lambda(M) = \sum_{i=1}^{g} k_i \deg(f_i) \quad \text{and} \quad \mu(M) = \sum_{j=1}^{h} \mu_j$$

are known as the λ-invariants and μ-invariants of M, respectively.

REMARK 2.3.8. The λ-invariant of a finitely generated Λ-module M is the $\mathbb{Z}_p$-rank of the Λ-torsion subgroup of M.

DEFINITION 2.3.9. The characteristic polynomial of a finitely generated Λ-module M which is pseudo-isomorphic to a module as in (2.3.2) Theorem 2.3.6 is defined to be $p^{\mu(M)} \prod_{i=1}^{g} f_i^{k_i}$, and the characteristic ideal $\mathrm{char}(M)$ is the ideal of Λ which it generates.

DEFINITION 2.3.10. For a Λ-module M, we let M^ι denote the Λ-module that is M as a pro-p group and upon which $f \in \Lambda$ acts as multiplication by $\iota(f)$ on M, where

$$\iota(f)(T) = f((T+1)^{-1} - 1).$$

The following can be seen through a bit of commutative algebra.

PROPOSITION 2.3.11 (IWASAWA). *The Λ-modules X_∞^ι and $A_\infty^\vee$ are pseudo-isomorphic.*

In particular, we have $\mu(X_\infty) = \mu(A_\infty^\vee)$ and $\lambda(X_\infty) = \lambda(A_\infty^\vee)$, while if f is the characteristic polynomial of X_∞, then $\iota(f)$ is the characteristic polynomial of $A_\infty^\vee$.

The structure theorem for finitely generated, torsion Λ-modules has direct consequences for the growth of the orders of the groups A_n. That is, Iwasawa proved the following [**Iwa1**].

THEOREM 2.3.12 (IWASAWA). *We have*

$$|A_{n+1}| = p^{p^n\mu+n\lambda+\nu}$$

for $n \geq 0$ sufficiently large, where $\mu = \mu(X_\infty)$, $\lambda = \lambda(X_\infty)$, and $\nu \in \mathbb{Z}$.

IDEA OF PROOF. We explain the idea and leave the details to the reader. In our case of interest, the map $(X_\infty)_{\Gamma^{p^n}} \to A_{n+1}$ between the Γ^{p^n}-coinvariant group of X_∞ (i.e., the largest quotient on which $\Gamma^{p^n} = 1 + p^{n+1}\mathbb{Z}_p$ acts trivially) is an isomorphism. This is a consequence of the facts that p is the unique prime over p in $F = \mathbb{Q}(\mu_p)$ and totally ramified in F_∞. (In general, it will have kernel and cokernel bounded in n.). Since X_∞ is pseudo-isomorphic to a direct sum as in (2.3.2), we again obtain a map between the Γ^{p^n}-coinvariant groups with kernel and cokernel bounded (and eventually stable) in n. These kernels and cokernels will contribute to the integer ν. The result is the reduced to a statement about the growth of coinvariant groups of quotients of Λ by principal ideals. For example, $\mathbb{F}_p[\![T]\!]/((T+1)^{p^n} - 1)$ is an $\mathbb{F}_p$-vector space of dimension p^n, explaining the occurrence of $p^n\mu$ in the exponent. □

Regarding the μ-invariant, Ferrrero and Washington proved the following theorem [**FeWa**].

THEOREM 2.3.13 (FERRERO-WASHINGTON). *The μ-invariant of X_∞ is zero.*

REMARK 2.3.14. The Ferrero-Washington theorem applies more generally to abelian fields F. Iwasawa conjectured that $\mu(X_\infty) = 0$ for all number fields F.

By class field theory, the group A_n is isomorphic to the Galois group of the maximal unramified abelian p-extension of F_n. It follows that X_∞ is continuously isomorphic to the Galois group of the maximal unramified abelian pro-p extension L_∞ of $F_\infty = \mathbb{Q}(\mu_{p^\infty})$.

The isomorphism $X_\infty \cong \mathrm{Gal}(L_\infty/F_\infty)$ is one of Λ-modules with respect to the continuous action of $\sigma \in \Gamma$ on $\tau \in \mathrm{Gal}(L_\infty/F_\infty)$ given by lifting σ to $\tilde{\sigma} \in \mathrm{Gal}(L_\infty/\mathbb{Q})$ and conjugating:

$$\sigma \cdot \tau = \tilde{\sigma}\tau\tilde{\sigma}^{-1}.$$

This is independent of the choice of $\tilde{\sigma}$ as X_∞ is abelian.

DEFINITION 2.3.15. We refer to the Λ-module $X_\infty \cong \mathrm{Gal}(L_\infty/F_\infty)$ as the unramified Iwasawa module over F_∞. The Λ-module A_∞ is called the p-part of the class group of F_∞.

Similarly, we may define the p-ramified Iwasawa module over F_∞ as follows.

DEFINITION 2.3.16. The p-ramified Iwasawa module $\mathfrak{X}_\infty$ is the Galois group of the maximal pro-p, unramified outside p (and any real places) extension of F_∞, which is a Λ-module under the continuous action of Γ given by lifting and conjugating.

REMARK 2.3.17. The Λ-rank of $\mathfrak{X}_\infty$ is $\frac{p-1}{2}$ (for $F = \mathbb{Q}(\mu_p)$).

Any $\mathbb{Z}_p$-module M with a commuting action of an involution (e.g., a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-module, considering the element $-1 \in \mathbb{Z}_p$) has a decomposition into (± 1)-eigenspaces (or plus and minus parts) for its action: let us write these as $M^\pm$ so that $M = M^+ \oplus M^-$. (Such a decomposition does not in general exist if $p = 2$, but we can still speak of plus and minus parts.)

The plus part $\mathfrak{X}_\infty^+$ is in fact torsion. In fact, Kummer theory yields the following theorem of Iwasawa [**Iwa2**]. Recall that $\mathbb{Z}_p(1)$ is the compact $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-module (resp., $\mathbb{Z}_p[\![G_\mathbb{Q}]\!]$-module) that is $\mathbb{Z}_p$ as a compact $\mathbb{Z}_p$-module and upon which $a \in \mathbb{Z}_p^\times$ (resp., $\sigma \in G_\mathbb{Q}$) acts by multiplication by a (resp., by $\chi_p(\sigma)$).

THEOREM 2.3.18 (IWASAWA). *We have $\mathfrak{X}_\infty^+ \cong (A_\infty^-)^\vee(1)$ as $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-modules.*

PROOF. Any p-ramified Kummer extension of F_n that is cyclic of degree dividing p^n is generated by the p^nth root of an element $a \in F_n^\times$ such that $a\mathbb{Z}[\mu_{p^n}]$ is the product of a power of the prime over p and the p^nth power of a fractional ideal prime to p. Let $\mathcal{B}_n$ denote the subgroup of $F_n^\times$ consisting of such elements. By Kummer theory, we have

$$\mathcal{B}_n/(\mathcal{B}_n \cap F_n^{\times p^n}) \cong \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n}),$$

where $\mathfrak{X}_n$ is the Galois group of the maximal p-ramified extension of F_n. Our description of $\mathcal{B}_n$ therefore provides an exact sequence

$$0 \to \mathcal{E}_n/\mathcal{E}_n^{p^n} \to \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n}) \to A_n[p^n] \to 0, \tag{2.3.3}$$

where $\mathcal{E}_n = \mathbb{Z}[\frac{1}{p}, \mu_{p^n}]^\times \otimes_\mathbb{Z} \mathbb{Z}_p$ is the p-completion of the group of p-units in F_n. (With the identification just described, the surjection in the sequence takes $a \in \mathcal{B}_n$ to the class of the fractional ideal $\mathfrak{a}$ such that $\mathfrak{a}^{p^n} = a\mathbb{Z}[\frac{1}{p}, \mu_{p^n}]$.)

We consider the direct limit over n of the minus parts of the sequences (2.3.3). Note that $\mathcal{E}_n^- \cong (\mathcal{E}_n/\mathcal{E}_n^{p^n})^- \cong \mu_{p^n}$, and $\varinjlim \mu_{p^n} = 0$ here, since the maps in the direct system of these groups are p-power maps. Since

$$\varinjlim_n \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n})^- \cong \varinjlim_n (\mathfrak{X}_n^+/p^n\mathfrak{X}_n^+)^\vee(1) \cong \left(\varprojlim_n \mathfrak{X}_n^+/p^n\mathfrak{X}_n^+\right)^\vee(1) \cong (\mathfrak{X}_\infty^+)^\vee(1)$$

and $\varinjlim A_n[p^n]^- \cong A_\infty^-$, we obtain the result. □

REMARK 2.3.19. For an arbitrary CM field F and any prime p, the plus part is again torsion, and if F contains μ_q, then Theorem 2.3.18 holds for F_∞.

COROLLARY 2.3.20. *Let f denote the characteristic polynomial of X_∞^-. Then the characteristic polynomial of $\mathfrak{X}_\infty^+$ is $f(\upsilon(T+1)^{-1} - 1)$, where $\upsilon = \chi_p(\gamma)$.*

Iwasawa showed that X_∞^- has no nonzero finite Λ-submodule [**Iwa2**]. Between this and the Ferrero-Washington theorem, we have the following.

PROPOSITION 2.3.21. *The Λ-module X_∞^- is p-torsion free.*

REMARK 2.3.22. What we shall be most interested in below for $F = \mathbb{Q}(\mu_p)$ is a finer decomposition of $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-modules. That is, if M is such a module, then as a $\mathbb{Z}_p[(\mathbb{Z}/p\mathbb{Z})^\times]$-module, it has a decomposition into eigenspaces as before. Each of these eigenspaces $M^{(i)}$ is then a Λ-module.

2.4. Kubota-Leopoldt p-adic L-functions

We have the following congruences among generalized Bernoulli numbers.

PROPOSITION 2.4.1. *For positive integers j and k with $j \equiv k \bmod p^{r-1}(p-1)$ for some $r \geq 1$, and a $\overline{\mathbb{Q}}_p$-valued primitive Dirichlet character χ with $\chi(-1) = (-1)^j$ and such that $\chi\omega^j \neq 1$, we have*

$$(1 - \chi(p)p^{j-1})\frac{B_{j,\chi}}{j} \equiv (1 - \chi(p)p^{k-1})\frac{B_{k,\chi}}{k} \bmod p^r$$

and for any $i \geq 1$, we have

$$\frac{B_{j,\chi}}{j} \equiv \frac{B_{i,\chi\omega^{j-i}}}{i} \bmod p.$$

These congruences can be used in proving the existence and continuity of p-adic L-functions, as constructed by Kubota and Leopoldt [**KuLe**].

THEOREM 2.4.2 (KUBOTA-LEOPOLDT). *Let χ be an even primitive Dirichlet character of conductor Mp^r for some $r \geq 0$ and $M \geq 1$ prime to p. Given an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$, there exists a unique p-adic analytic (aside from $s = 1$ if $\chi = 1$, where it has a pole with residue $1 - p^{-1}$) function $L_p(\chi, s)$ on $\mathbb{Z}_p$ satisfying*

$$L_p(\chi, 1 - i) = (1 - \chi\omega^{-i}(p)p^{i-1})L(\chi\omega^{-i}, 1 - i)$$

for all $i \geq 1$.

DEFINITION 2.4.3. The function $L_p(\chi, s)$ is the Kubota-Leopoldt p-adic L-function of χ.

Let us indicate briefly how the Kubota-Leopoldt p-adic L-function can be constructed.

DEFINITION 2.4.4. For each $n \geq 1$, the nth Bernoulli polynomial $B_n(X) \in \mathbb{Q}[x]$ is defined by the power series expansion

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!},$$

EXAMPLE 2.4.5. We have $B_0(X) = 1$, $B_1(X) = X - \frac{1}{2}$, and $B_2(X) = X^2 - X + \frac{1}{6}$.

The relationship between Bernoulli polynomials and Bernoulli numbers is seen in the following lemma.

LEMMA 2.4.6. *If χ is a Dirichlet character of modulus (dividing) N, then*

$$B_{k,\chi} = N^{k-1}\sum_{a=1}^{N} \chi(a)B_k\left(\frac{a}{N}\right).$$

Using the Bernoulli polynomials, we can construct a distribution on $\mathbb{Q}/\mathbb{Z}$ known as the Bernoulli distribution. That is, these polynomials have the property that

$$M^{k-1}B_k\left(\frac{a}{M}\right) = \sum_{j=0}^{N/M-1} N^{k-1}B_k\left(\frac{a + jM}{N}\right)$$

for M dividing N.

SKETCH OF CONSTRUCTION OF p-ADIC L-FUNCTIONS. For simplicity of presentation, we focus on the case that our Dirichlet character has conductor an odd prime p, i.e., is an even power of ω. Form the modified Stickelberger elements

$$\Theta_n = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \left(\frac{a}{p^n} - \frac{1}{2}\right)[a]^{-1} \in \mathbb{Q}[(\mathbb{Z}/p^n\mathbb{Z})^\times]$$

out of the values $B_1(\frac{a}{p^n}) = \frac{a}{p^n} - \frac{1}{2}$. These elements are compatible under the natural projection maps and thus define in the inverse limit an element Θ_∞ of the total quotient ring $\mathcal{Q}$ of $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$.

We can take the projection of Θ_∞ to $\mathcal{Q}^{(1-k)}$, obtaining an element $\Theta_\infty^{(k)}$. Identifying $\gamma - 1$ with T and Δ with $\mu_{p-1}(\mathbb{Z}_p)$, we have

$$\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^{(1-k)} \cong \Lambda[\Delta]^{(1-k)} \cong \Lambda \cong \mathbb{Z}_p[\![T]\!],$$

so $\Theta_\infty^{(k)}$ lies in the quotient field of Λ.

For $k \not\equiv 0 \bmod p-1$, the element $\Theta_\infty^{(k)}$ lies in $\mathbb{Z}_p[\![T]\!]$. For $k \equiv 0 \bmod p-1$, it can be made to have integral coefficients by multiplication by $[v] - v$, which is sufficient to avoid convergence issues, by premultiplying and then multiplying back in the factor after evaluation. (For such k, the numerator of $\Theta_\infty^{(k)}$ is a unit power series.) The p-adic L-function for the character ω^k is then defined by

$$L_p(\omega^k, s) = -\Theta_\infty^{(k)}(v^s - 1)$$

for $s \in \mathbb{Z}_p$. □

2.5. The Iwasawa main conjecture

We present the classical Iwasawa main conjecture here over the cyclotomic $\mathbb{Z}_p$-extension of $F = \mathbb{Q}(\mu_p)$, for p odd, which is a theorem of Mazur and Wiles. This conjecture was stated more generally for any abelian field F, and it was proven by Mazur and Wiles for odd p [**MaWi1**]. Wiles treated the case $p = 2$, as well as a generalization of the main conjecture to totally real fields [**Wil2**]. The only real difference from the case of $\mathbb{Q}(\mu_p)$ in the statement for more general abelian fields is the need for a discussion of "eigenspaces" for more general finite order characters. The reader might therefore be able to determine the appropriate formulation.

Let us set $f_k = -\Theta_\infty^{(k)}$ for $k \not\equiv 0 \bmod p-1$ so that

$$f_k(v^s - 1) = L_p(\omega^k, s).$$

For $k \equiv 0 \bmod p-1$, we set $f_k = 1$. Iwasawa stated in [**Iwa4**] and proved in [**Iwa5**] the following theorem under the condition that $A^{(k)} = 0$ (where $A = A_1$ is the p-part of the class group of F). It is alternately known as the Iwasawa main conjecture, Iwasawa's main conjecture, and the main conjecture of Iwasawa theory, or simply the main conjecture.

THEOREM 2.5.1 (IWASAWA MAIN CONJECTURE, MAZUR-WILES). *Let k be an even integer. Then*

$$\mathrm{char}(X_\infty^{(1-k)}) = (f_k).$$

REMARK 2.5.2. The analytic class number tells us that the orders $h_n^{(p)}$ of the groups in the tower can be expressed in terms of products of Bernoulli numbers. From this, one can conclude that

$$\lambda(X_\infty^-) = \sum_{j=0}^{(p-3)/2} \lambda(\Lambda/(f_{2j})),$$

as well as the corresponding equality of μ-invariants (which we already know to equal zero by the Ferrero-Washington theorem). Consequently, to prove the main conjecture, it suffices to show either that $\mathrm{char}(X_\infty^{(1-k)})$ divides (f_k) for all even k, or vice versa.

The approach to the main conjecture due to Mazur and Wiles, which exploits the geometry of modular curves near the cusps, is to show that (f_k) divides $\mathrm{char}(X_\infty^{(1-k)})$.

REMARK 2.5.3. Rubin gave another proof of the main conjecture by exhibiting the opposite divisibility, bounding the size of the unramified Iwasawa module by exploiting the method of Euler systems of Thaine and Kolyvagin (see the lectures of D. Loeffler and S. Zerbes). This uses norm relations among cyclotomic units in auxiliary cyclotomic extensions of the fields $\mathbb{Q}(\mu_{p^n})$. Our focus in these notes is on the approach of Mazur and Wiles. It's important, however, to be aware that analogues of the analytic class number formula are not generally available for the Selmer groups of Galois representations, and so proofs of more general main conjectures for these objects have required both the study of higher-dimensonal Galois representations and congruences and the method of Euler systems.

Let us next discuss some equivalent formulations of the Iwasawa main conjecture. The first describes the characteristic ideal of the p-ramified Iwasawa module $\mathfrak{X}_\infty$. Set

$$g_k(T) = f_k(\upsilon(1+T)^{-1} - 1),$$

so

$$g_k(\upsilon^s - 1) = L_p(\omega^k, 1-s)$$

for $k \not\equiv 0 \bmod p-1$. Then the main conjecture is equivalent to the following statement.

THEOREM 2.5.4 (IWASAWA MAIN CONJECTURE, VERSION 2). *Let k be an even integer. Then*

$$\mathrm{char}(\mathfrak{X}_\infty^{(k)}) = (g_k).$$

A third equivalent version of the main conjecture can be given in terms of the norm compatible sequences in the p-completions of the unit groups of the fields F_n. Let

$$\mathcal{E}_n = \mathbb{Z}_p[\tfrac{1}{p}, \mu_{p^n}]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

and set $\mathcal{E}_\infty = \varprojlim_n \mathcal{E}_n$, the transition maps being induced by the norm maps of the field extensions. Similarly, let $\mathcal{U}_n$ denote the pro-p completion of $\mathbb{Q}_p(\mu_{p^n})^\times$, and set $\mathcal{U}_\infty = \varprojlim_n \mathcal{U}_n$. Class field theory provides an exact sequence

$$0 \to \mathcal{E}_\infty \to \mathcal{U}_\infty \to \mathfrak{X}_\infty \to X_\infty \to 0,$$

the first map being injective by a theorem known as the weak Leopoldt conjecture (see the lectures of J. Coates).

Let $\mathcal{C}_n$ denote the subgroup of $\mathcal{E}_n$ topologically generated by the cyclotomic p-units $1-\zeta_{p^n}^i$ with $p \nmid i$, and set $\mathcal{C}_\infty = \varprojlim_n \mathcal{C}_n$. The abelian pro-$p$ group $\mathcal{E}_\infty/\mathcal{C}_\infty$ is a Λ-torsion module that is fixed under the action of complex conjugation.

The group $(\mathcal{U}_\infty/\mathcal{C}_\infty)^+$ has a very fascinating description by a result of Iwasawa. We describe Coleman's approach to it [**Col2**]. It begins with his construction of Coleman power series [**Col1**].

THEOREM 2.5.5 (COLEMAN). *Given a norm compatible sequence $u = (u_n)_n \in \mathcal{U}_\infty$, there exists a unique power series $f \in \mathbb{Z}_p[\![T]\!]$ with $f(\zeta_{p^n}-1) = u_n$ for all $n \geq 1$.*

The power series g_u attached to $u \in \mathcal{U}_\infty$ by Coleman's theorem is known as the Coleman power series of u. The modified logarithm

$$\ell_p(g_u) = \log(f(T)) - \frac{1}{p}\log(f((T+1)^p - 1))$$

of this f lies in $\mathbb{Z}_p[\![T]\!]$ as well. The completed group ring $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ acts on $\mathbb{Z}_p[\![T]\!]$ via the continuous $\mathbb{Z}_p$-linear action under which $a \in \mathbb{Z}_p^\times$ maps T to $(1+T)^a - 1$. We then define an injective homomorphism

$$\phi\colon \mathcal{U}_\infty \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$$

on $u \in \mathcal{U}_\infty$ by letting $\phi(u) \in \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ be the unique element such that $\phi(u)\cdot T = \ell_p(g_u)$. On the ω^k-eigenspace for $k \not\equiv 0 \bmod p-1$, the homomorphism has image in $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$. Coleman proved that

$$\phi((1-\zeta_{p^n})_n) = \Theta_\infty.$$

Consequently, we have the following theorem, originally due to Iwasawa [**Iwa3**].

THEOREM 2.5.6 (IWASAWA). *Let k be an even integer. Then there is a canonical isomorphism of Λ-modules*

$$\mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \cong \Lambda/(f_k).$$

For an even integer k, we have an exact sequence

$$0 \to \mathcal{E}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \to \mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \to \mathfrak{X}_\infty^{(k)} \to X_\infty^{(k)} \to 0 \tag{2.5.1}$$

of finitely generated Λ-torsion modules. The alternating product of characteristic ideals in an exact sequence of such modules is the unit ideal. By this and Theorem 2.5.6, we have the following equivalent form of the main conjecture.

THEOREM 2.5.7 (IWASAWA MAIN CONJECTURE, VERSION 3). *Let k be an even integer. Then the characteristic ideals of $\mathcal{E}_\infty^{(k)}/\mathcal{C}_\infty^{(k)}$ and $X_\infty^{(k)}$ are equal.*

Greenberg conjectured the following weaker form of Vandiver's conjecture [**Gre2**].

CONJECTURE 2.5.8 (GREENBERG). *The Iwasawa module X_∞^+ is finite.*

EXERCISE 2.5.9. Greenberg's conjecture has equivalent formulations in the statements that $A_\infty^+ = 0$ and that $\mathcal{E}_\infty = \mathcal{C}_\infty$.

REMARK 2.5.10. In fact, Greenberg conjectured that X_∞^+ is finite with F_∞ replaced by the cyclotomic $\mathbb{Z}_p$-extension of any totally real or CM field, in which case X_∞^+ is not in general zero. The first occurrence of the Iwasawa main conjecture for general abelian fields in print is found in a paper of Greenberg's [**Gre1**].

From Theorem 2.5.6, we conclude the following.

COROLLARY 2.5.11. *If Greenberg's conjecture that $X_\infty^{(k)}$ is finite holds, then the Iwasawa main conjecture holds for $X_\infty^{(1-k)}$, and the latter Λ-module is pseudo-cyclic, i.e., pseudo-isomorphic to $\Lambda/(f_k)$.*

REMARK 2.5.12. Iwasawa had proven that $X_\infty^{(1-k)}$ is cyclic if $X_\infty^{(k)} = 0$ in [**Iwa5**]. Coates and Lichtenbaum conjectured that $X_\infty^{(k)}$ is pseudo-cyclic (in fact, for even eigenspaces of general abelian fields of degree prime to p) [**CoLi**].

Finally, we remark that as a consequence of the main conjecture, Mazur and Wiles were able to prove a precise formula for the order of the odd eigenspaces of $A = A_1$. This provides a direct refinement of the Herbrand-Ribet theorem.

THEOREM 2.5.13 (MAZUR-WILES). *For every even integer k, we have*

$$|A^{(1-k)}| = p^{v_p(B_{1,\omega^{k-1}})},$$

where v_p denotes the p-adic valuation.

CHAPTER 3

Theory of modular forms

In this chapter, we briefly review the theory of modular curves and modular forms, tailored to our study. Our interest in these notes is in modular curves as they apply to the study of the arithmetic of cyclotomic fields.

We can only hope in these subsections to give an overly short and hurried description of the theory, presuming that the reader is already somewhat familiar with the subject, as we shall assume more completely in the lectures themselves. We recommend that the reader unfamiliar with the subject consult a good textbook (e.g., [**DiSh, Lan, Shi2, Hid4**]) and other available sources rather than to attempt to gain anything close to a full understanding solely through these notes.

3.1. Modular curves over $\mathbb{C}$

The group $\mathrm{GL}_2(\mathbb{R})_+$ of invertible matrices with positive determinant acts on the complex upper half-plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

by Möbius transformations: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$, then

$$\gamma \cdot z = \frac{az+b}{cz+d} \in \mathbb{H}.$$

This group acts by the same formula on $\mathbb{R} \cup \{\infty\}$, but in fact what we shall be interested in is $\mathbb{Q} \cup \{\infty\}$, which is also preserved under the action.

Definition 3.1.1. The extended upper half-plane is $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

We give $\mathbb{H}^*$ a topology extending the usual Euclidean topology on $\mathbb{H}$ by declaring a basic open neighborhood of a rational number to be the set consisting of said point and an open disk tangent to it and a basic open neighborhood of infinity to be the set consisting of it and all complex numbers with imaginary part at least some fixed nonnegative number. The group $\mathrm{GL}_2(\mathbb{Q})_+ = \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2(\mathbb{R})_+$ then acts continuously on $\mathbb{H}^*$.

Definition 3.1.2. Let N be a positive integer.

(1) The principal congruence subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, i.e., the matrices congruent to 1 modulo N.

(2) A congruence subgroup of level N is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ but not $\Gamma(M)$ for any proper divisor M of N.

(3) The congruence subgroup $\Gamma_0(N)$ is the subgroup of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that are upper-triangular modulo N.

(4) The congruence subgroup $\Gamma_1(N)$ is the subgroup of matrices in $\Gamma_0(N)$ that are unipotent modulo N.

DEFINITION 3.1.3. For a congruence subgroup Γ, we have the open and closed modular curves $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ and $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$, respectively. The cusps of $X(\Gamma)$ are the points of the finite set

$$C(\Gamma) = X(\Gamma) - Y(\Gamma) = \Gamma\backslash(\mathbb{Q} \cup \{\infty\}).$$

DEFINITION 3.1.4. For $j \in \{0, 1\}$, we set $Y_j(N) = Y(\Gamma_j(N))$ and $X_j(N) = X(\Gamma_j(N))$ for $j \in \{0, 1\}$, and we let $C_j(N)$ denote their sets of cusps.

REMARK 3.1.5. The closed curves are compactifications of the open curves. The modular curves can be given the structure of Riemann surfaces, taking care of the charts around the cusps and the elliptic points, the latter being the classes of the points i, $e^{\pi i/3}$, and $e^{2\pi i/3}$ in a manner that we omit here.

For the most part, we will be concerned with the modular curve $X_1(N)$. The following lemma describes its cusps.

LEMMA 3.1.6. *Two fractions $\frac{a}{c}$ and $\frac{a'}{c'}$ in reduced form represent the same cusp of $X_1(N)$ if and only if $c \equiv \pm c' \bmod N$ and $a \equiv \pm a' \bmod (c, N)$ for the same choice of sign.*

Modular curves have fundamental domains in $\mathbb{H}^*$, which (we shall not define but) in particular are connected subsets of $\mathbb{H}^*$ that project bijectively onto $X(\Gamma)$.

EXAMPLE 3.1.7. The set $\{z \in \mathbb{H} \mid \mathrm{Re}(z) \le \frac{1}{2},\ |z| \ge 1\} \cup \{\infty\}$ is the closure of a fundamental domain for $X(\mathrm{SL}_2(\mathbb{Z}))$.

We next turn to Hecke operators. Consider the divisor group $\mathrm{Div}(X_1(N))$ that is the free abelian group on the points of $X_1(N)$. Note that the action of $\mathrm{GL}_2(\mathbb{Q})_+$ on $X_1(N)$ extends additively to an action on divisors.

DEFINITION 3.1.8. For $j \in \mathbb{Z}$ prime to the level N, the diamond operator

$$\langle j \rangle \colon \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$$

is the map induced by the Möbius transformation associated to any matrix $\delta_j \in \Gamma_0(N)$ with lower right entry congruent to j modulo N. For j sharing a common divisor with N, we set $\langle j \rangle = 0$.

The nth Hecke operators T_n for $n \ge 1$ may be defined via correspondences. That is, we consider the correspondence on the level N modular curve that is represented by the diagram

$$\begin{array}{ccc} & X(\Gamma_1(N) \cap \Gamma_0(Nn)) & \\ {\scriptstyle \epsilon_1}\swarrow & & \searrow{\scriptstyle \epsilon_n} \\ X_1(N) & & X_1(N). \end{array} \tag{3.1.1}$$

For $d \ge 1$ (dividing n), the degeneracy map ϵ_d is induced by the map $d \colon \mathbb{H}^* \to \mathbb{H}^*$ given by multiplication by d.

DEFINITION 3.1.9. For $n \geq 1$, the nth Hecke operator $T_n \colon \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$ is the unique homomorphism that on the class $\{x\}$ of $x \in X_1(N)$ is given by

$$T_n(\{x\}) = \sum_{y \in \epsilon_1^{-1}(x)} \{\epsilon_n(y)\},$$

That is, T_n is given by pulling back by ϵ_1 and then pushing forward by ϵ_n.

EXERCISE 3.1.10. For a prime p, the application of T_p to a $\mathbb{C}$-point represented by $z \in \mathbb{H}^*$ is the divisor given by the sum over the application to z of the right coset representatives of the $\Gamma_1(N)$-double cosets of the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. One set of such representatives consists of the matrices $\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)$ for $0 \leq j \leq p-1$ and, if $p \nmid N$, the matrix $\delta_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (given a choice of δ_p as above).

REMARK 3.1.11. It may seem a bit silly at first, but we may also think of $\langle j \rangle$ for j prime to N as defined by a correspondence $X_1(N) \xleftarrow{\mathrm{id}} X_1(N) \xrightarrow{\delta_j} X_1(N)$ given by pulling back by the identity and pushing forward by the action of δ_j.

EXERCISE 3.1.12. The Hecke operators and the diamond operators defined above are all mutually commutative.

Now we turn to general Hecke operators.

EXERCISE 3.1.13. For a prime p and $n \geq 1$, the p^{n+1}th Hecke operator satisfies

$$T_{p^{n+1}} = T_{p^n} T_p - p\langle p \rangle T_{p^{n-1}},$$

where $T_1 = 1$. Moreover, if m and n are relatively prime postiive integers, then $T_{mn} = T_m T_n$.

Given an operator defined by a correspondence, we may define its transpose as the operator given by switching the order of the two arrows in the diagram defining it.

DEFINITION 3.1.14. The nth adjoint Hecke operator T_n^* is the transpose of T_n, and the diamond operator $\langle j \rangle^*$ is the transpose of $\langle j \rangle$ for j prime to N (and zero otherwise).

One might note that $\langle j \rangle^* = \langle j \rangle^{-1}$ for j prime to N.

REMARK 3.1.15. Alternatively, the adjoint operator T_n^* to T_n is given by $T_n^* = w_N T_n w_N^{-1}$, where w_N is the Atkin-Lehner operator induced by the action of the matrix $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. We also have $\langle j \rangle^* = w_N \langle j \rangle w_N^{-1}$.

3.2. Moduli-theoretic interpretation

The modular curves we have defined are not just complex manifolds, but in fact varieties, cut out by polynomial equations. Even better, for small enough Γ, we can define them as the $\mathbb{C}$-points of schemes over $\mathbb{Z}$.

For $N \geq 4$, the modular curve $Y_1(N)$ is the moduli space with S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S equal to the set of isomorphism classes of pairs (E, P), where E is an elliptic curve over S and P is a point of E of order N, which we take to mean given by an injective morphism $(\mathbb{Z}/N\mathbb{Z})_{/S} \to E[N]_{/S}$ of S-schemes from the constant group scheme $\mathbb{Z}/N\mathbb{Z}$ over S to the

subgroup scheme $E[N]$ of E of N-torsion points, viewed as an S-scheme. In fact, it is a fine moduli scheme, which is to say that it represents the functor that takes S to the aforementioned set, and it is smooth of finite type over $\mathbb{Z}[\frac{1}{N}]$.

Similarly, $Y_0(N)$ over $\mathbb{Z}[\frac{1}{N}]$ is the "course" moduli space with S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S equal to the set of isomorphism classes (E, C), where E is an elliptic curve over S and C is a cyclic subgroup of order N, i.e., an S-subgroup scheme of $E[N]$ that is (étale) locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})_{/S}$. (We shall not define these notions more precisely.)

REMARK 3.2.1. There is an implicit choice of "model" made here so that we can define $Y_1(N)$ over a ring without Nth roots of unity, i.e., we take a constant subscheme as part of the moduli data, rather than the S-scheme $(\mu_N)_{/S}$.

The closed modular curves $X_1(N)$ and $X_0(N)$ of level N are smooth, proper curves over $\mathbb{Z}[\frac{1}{N}]$ containing the corresponding open modular curve as an open subscheme. These again have a moduli interpretation using generalized elliptic curves in place of elliptic curves, which is necessary at the cusps [**DeRa**]. These cusps are points defined over cyclotomic integer rings with N inverted.

REMARK 3.2.2. Our choice of model insures that the cusp 0 on $X_1(N)$ is rational, defined over $\operatorname{Spec}\mathbb{Z}[\frac{1}{N}]$, whereas ∞ is a $\operatorname{Spec}\mathbb{Z}[\mu_N, \frac{1}{N}]^+$-point of $X_1(N)$.

REMARK 3.2.3. In fact, the modular curves $Y_1(N)$ and $X_1(N)$ can be defined over $\mathbb{Z}$ by taking the normalizations of the affine and projective j-lines over $\mathbb{Z}$ inside the $\mathbb{Z}[\frac{1}{N}]$-schemes, though we must modify the moduli interpretation, using Drinfeld level structures in the place of points [**KaMa**]. These schemes are still flat over $\mathbb{Z}$, though no longer étale. (See [**Con**] for more information, stronger results, and a much more careful treatment.)

The Hecke operators on the group $\operatorname{Div}(X_1(N)(S))$ of formal sums of S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S are also defined via correspondences as in (3.1.1), i.e., T_n is defined as $(\epsilon_n)_*\epsilon_1^*$ once we define degeneracy maps. The diamond operator $\langle j\rangle$ is defined more simply by

$$\langle j\rangle(E, P) = (E, jP).$$

On S-points of the open modular curves for a $\mathbb{Z}[\frac{1}{Nn}]$-scheme S, the degeneracy maps have the following description. Let d divide n. For an elliptic curve E over S, a point P of order N on E, and cyclic subgroup C of E of order Nn containing P, in the senses defined above, the triple (E, P, C) defines a point of $X(\Gamma_1(N) \cap \Gamma_0(n))(S)$. The degeneracy map

$$\epsilon_d \colon X(\Gamma_1(N) \cap \Gamma_0(n)) \to X_1(N)$$

for d dividing n is defined on the S-point (E, P, C) by

$$\epsilon_d(E, P, C) = (E/C', P' + C'),$$

where C' is the cyclic subgroup scheme of order d in C and P' is any point of E with $P = dP'$. The resulting formula for $(\epsilon_n)_*\epsilon_1^*$ works for points of any $\mathbb{Z}[\frac{1}{N}]$-scheme S.

THEOREM 3.2.4 (KATZ-MAZUR). *There exists a smooth $\mathbb{Z}[\frac{1}{N}]$-scheme called the universal elliptic curve $\mathcal{E}_1(N)$ over $Y_1(N)$, the fiber above a point $(E,P) \in Y_1(N)(S)$ being the elliptic curve E itself.*

REMARK 3.2.5. The scheme $\mathcal{E}_1(N)$ is an open subscheme of a universal generalized elliptic curve over $X_1(N)$, which has generalized elliptic curves as fibers.

For later use, we recall theta functions and Siegel units (see [**Kat**, Section 1]).

DEFINITION 3.2.6. Let $\mathcal{E} = \mathcal{E}_1(N)$. For an integer $c > 1$ and prime to 6, the theta function

$$ {}_c\theta \in \mathcal{O}(\mathcal{E}\backslash\mathcal{E}[c])^\times $$

is the unique element with Cartier divisor $c^2(0) - \mathcal{E}[c]$ that is invariant under norm maps attached to multiplication by a, for a prime to c.

EXERCISE 3.2.7. Let $c, d > 1$ be prime to 6. Then $d^*(\theta_c)\theta_c^{-d^2} = c^*(\theta_d)\theta_d^{-c^2}$ in $\mathcal{O}(\mathcal{E}\backslash\mathcal{E}[cd])^\times$.

DEFINITION 3.2.8. Let $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, and let $c \geq 1$ be prime to $6N$. The Siegel unit ${}_cg_u \in \mathcal{O}(Y_1(N))^\times$ is the pullback of ${}_c\theta$ by the section of $\mathcal{E}_1(N) \to X_1(N)$ taking $(E,P) \in X_1(N)(S)$ for a $\mathbb{Z}[\frac{1}{N}]$-scheme S to the point uP on its fiber E in $\mathcal{E}_1(N)(S)$.

DEFINITION 3.2.9. For $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, the Siegel unit

$$ g_u \in \mathcal{O}(Y_1(N))^\times \otimes_{\mathbb{Z}} \mathbb{Z}[\tfrac{1}{6N}] $$

is the unique element with the property that for any $c > 1$ prime to $6N$, we have

$$ {}_cg_u = \frac{g_u^{c^2}}{g_{cu}}. $$

REMARK 3.2.10. Over $\mathbb{C}$, the Siegel unit g_u has the q-expansion

$$ (-\zeta_N)^{-\frac{u}{2}} q^{\frac{1}{12}} \prod_{n=0}^{\infty}(1-q^n\zeta_N^u) \prod_{n=1}^{\infty}(1-q^n\zeta_N^{-u}). \tag{3.2.1} $$

(The power of $-\zeta_N$ is placed here somewhat artificially, but one gets the q-expansion of ${}_cg_u$ without tensoring with $\mathbb{Z}[\frac{1}{6N}]$ from it.)

3.3. Modular forms

DEFINITION 3.3.1. A modular form of weight k and level N is a holomorphic function $f\colon \mathbb{H}^* \to \mathbb{C}$ such that

$$ f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) $$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ and $z \in \mathbb{H}^*$.

Since $f(z+1) = f(z)$ for all $z \in \mathbb{H}$, to say that f is holomorphic at ∞ is to say that it has a Fourier expansion in $q = e^{2\pi iz}$ (or q-expansion) given by

$$ f(q) = \sum_{n=0}^{\infty} a_n(f) q^n \tag{3.3.1} $$

for some $a_n(f) \in \mathbb{C}$. The $a_n(f)$ are known as its Fourier coefficients. A modular form f is uniquely determined by its Fourier expansion.

DEFINITION 3.3.2. If a modular form f vanishes on $\mathbb{Q} \cup \{\infty\}$, then f is said to be a cusp form.

If f is a cusp form, then $a_0(f) = 0$, though the converse need not hold if its level is greater than 1.

DEFINITION 3.3.3. We let $M_k(N)$ (resp., $S_k(N)$) denote the $\mathbb{C}$-vector space of modular forms (resp., cusp forms) of weight k and level N.

The space $M_k(N)$ breaks up into a direct sum of subspaces corresponding to the Dirichlet characters of modulus N.

DEFINITION 3.3.4. For a character $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, we define the subspace $M_k(N, \chi)$ of modular forms with Nebentypus (or character) χ to be the set of $f \in M_k(N)$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \chi(d) f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. We set

$$S_k(N, \chi) = S_k(N) \cap M_k(N, \chi).$$

The following is then easily verified.

LEMMA 3.3.5. *We have*

$$M_k(N) = \bigoplus_\chi M_k(N, \chi) \quad \text{and} \quad S_k(N) = \bigoplus_\chi S_k(N, \chi),$$

where the direct sums are taken over $\mathbb{C}$-valued characters χ of $(\mathbb{Z}/N\mathbb{Z})^\times$.

We mention a couple of constructions that are useful to us.

DEFINITION 3.3.6. For $f \in M_k(N)$, the L-function $L(f, s)$ is the analytic continuation to $\mathbb{C}$ of the L-series

$$L_p(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}$$

that converges uniformly for $\mathrm{Re}(s) > k$ (or $\frac{k}{2} + 1$ if f is a cusp form). If χ is a Dirichlet character, we may define $L_p(f, \chi, s)$ as the analytic continuation of $\sum_{n=1}^{\infty} a_n(f)\chi(n)n^{-s}$.

EXAMPLE 3.3.7. The Eisenstein series E_k has L-function $L(E_k, s) = \zeta(s)\zeta(s-k+1)$.

We next explore the action of Hecke operators on spaces of modular forms. For this, we make the following definition.

DEFINITION 3.3.8. The group $\mathrm{GL}_2(\mathbb{Q})_+$ acts on $f \in M_k(N)$ on the right by

$$(f|_\gamma)(z) = (cz+d)^{-k} (\det \gamma)^{k-1} f(\gamma z)$$

for $\gamma \in \mathrm{GL}_2(\mathbb{Q})_+$.

This action induces an action of the operator corresponding to the double coset $\Gamma_1(N)\gamma\Gamma_1(N)$ which is given by summing over the applications of the matrices representing the right cosets in its decomposition.

DEFINITION 3.3.9. For $n \geq 1$, the nth Hecke operator T_n on $M_k(N)$ is the $\Gamma_1(N)$-double coset operator associated to $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$.

Diamond operators $\langle j \rangle$ on $M_k(N)$ are defined by the action of δ_j. We have

$$M_k(N, \chi) = \{f \in M_k(N) \mid \langle j \rangle(f) = \chi(j)f\}.$$

We may define the action of general Hecke operators by the recursive formulas of Definition 3.1.13.

EXERCISE 3.3.10. For any prime p, the action of T_p is given on the Fourier expansion of $f \in M_k(N, \chi)$ for a Dirichlet character χ of modulus N is given by

$$a_n(T_p f) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f), \tag{3.3.2}$$

taking $a_{n/p} = 0$ if $p \nmid n$.

DEFINITION 3.3.11. We say that $f \in M_k(N)$ is an eigenform if it is an eigenform (i.e., eigenvector) for all of the Hecke operators T_n and diamond operators $\langle j \rangle$ simultaneously (this latter condition saying that $f \in M_k(N, \chi)$ for some χ).

EXERCISE 3.3.12. If f is an eigenform with $a_1(f) = 1$, then $T_n(f) = a_n(f)f$ for all $n \geq 1$.

DEFINITION 3.3.13. An eigenform with q-coefficient equal to 1 is said to be normalized.

EXAMPLE 3.3.14. Let χ be a p-adic Dirichlet character of of modulus N with $\chi(-1) = (-1)^k$. Suppose that $k > 2$ if $N = 1$. The weight k Eisenstein series $E_{k,\chi} \in M_k(N, \chi)$ with character χ is the level N eigenform

$$E_{k,\chi} = -\frac{B_{k,\chi}}{2k} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1}\chi(d)q^n.$$

REMARK 3.3.15. There is a complement to $S_k(N)$ in $M_k(N)$ with a basis consisting of slightly more general Eisenstein series (see [**DiSh**, Section 3]).

EXERCISE 3.3.16. If f is a normalized eigenform in $M_k(N, \chi)$, then the L-series $L(f, s)$ has an Euler product expansion

$$L(f, s) = \prod_{p \text{ prime}} (1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

DEFINITION 3.3.17. The Petersson inner product

$$\langle\ ,\ \rangle \colon M_k(N) \times S_k(N) \to \mathbb{C}$$

is the positive definite Hermitian pairing defined by

$$\langle f, g \rangle = \frac{1}{\mathrm{Vol}(X_1(N))} \int_{X_1(N)} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2},$$

where the integral is taken over $z = x + iy$ in a fundamental domain in $\mathbb{H}^*$ of the modular curve $X_1(N)$, and $\mathrm{Vol}(X_1(N))$ is the volume of this fundamental domain under the hyperbolic measure $y^{-2}dxdy$.

REMARK 3.3.18. The adjoint Hecke operator T_n^* on $S_k(N)$ is in fact adjoint to T_n under the Petersson inner product, hence its name. If n is prime to N, it satisfies $T_n^* = \langle n\rangle^{-1}T_n$. Recall that $\langle j\rangle^* = \langle j\rangle^{-1}$ for j prime to N.

Since the Hecke operators T_n for n prime to N are normal operators that commute with each other (and the diamond operators), they are simultaneously diagonalizable, and hence we have the following.

THEOREM 3.3.19. *The spaces $M_k(N)$ and $S_k(N)$ have bases consisting of eigenforms for all Hecke operators T_n with n prime to N.*

Next, reusing notation, let us consider degeneracy maps $\epsilon_d\colon X_1(Nn) \to X_1(N)$ for $d \geq 1$ dividing n. On $\mathbb{C}$-points, which is all we require here, ϵ_d is induced by multiplication-by-d on $\mathbb{H}^*$. The degeneracy maps induce degeneracy maps $\epsilon_d\colon M_k(N) \to M_k(Nn)$ on spaces of modular forms given by $\epsilon_d(f)(z) = f(dz)$. These clearly preserve the subspaces of cusp forms.

DEFINITION 3.3.20. The subspace of oldforms $M_k(N)^{\mathrm{old}}$ in $M_k(N)$ is the span of all images $\epsilon_1(M_k(Np^{-1}))$ and $\epsilon_p(M_k(Np^{-1}))$ for primes p dividing N.

DEFINITION 3.3.21. The new subspace $S_k(N)^{\mathrm{new}}$ of $S_k(N)$ is the orthogonal complement of $S_k(N)^{\mathrm{old}} = M_k(N)^{\mathrm{old}} \cap S_k(N)$ under the Petersson inner product.

DEFINITION 3.3.22. An eigenform in $S_k(N)$ is said to be a newform if lies in $S_k(N)^{\mathrm{new}}$ and is normalized, i.e., has q-coefficient 1.

EXERCISE 3.3.23. For an eigenform to be a newform, it suffices that it have primitive nebentypus.

THEOREM 3.3.24. *The space $S_k(N)^{\mathrm{new}}$ has a basis consisting of eigenforms.*

We can also consider forms with coefficients in a commutative ring A.

DEFINITION 3.3.25. We define $M_k(N, \mathbb{Z}) \subseteq M_k(N)$ to be the subset of modular forms with q-expansions having coefficients in $\mathbb{Z}$, and we let $S_k(N, \mathbb{Z})$ be its subgroup of cusp forms.

EXERCISE 3.3.26. The ranks of the groups of modular forms with $\mathbb{Z}$-coefficients agree with the dimensions of the vector spaces of modular forms over $\mathbb{C}$:

$$\mathrm{rank}_{\mathbb{Z}}\, M_k(N, \mathbb{Z}) = \dim_{\mathbb{C}} M_k(N) \quad \text{and} \quad \mathrm{rank}_{\mathbb{Z}}\, S_k(N, \mathbb{Z}) = \dim_{\mathbb{C}} S_k(N).$$

DEFINITION 3.3.27. For a commutative ring A (with 1), we set

$$M_k(N, A) = M_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A \quad \text{and} \quad S_k(N, A) = S_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A.$$

DEFINITION 3.3.28. The full modular Hecke algebra $\mathfrak{H}_k(N, A)$ of weight k and level N is the A-subalgebra of the A-linear endomorphisms of $M_k(N, A)$ generated by the diamond operators $\langle j \rangle$ with $j \in (\mathbb{Z}/N\mathbb{Z})^\times$ and the Hecke operators T_n for $n \geq 1$. The cuspidal Hecke algebra $\mathfrak{h}_k(N, A)$ of weight k and level N is the image of $\mathfrak{H}_k(N, A)$ in $\mathrm{End}_A(S_k(N, A))$ upon restriction. If $A = \mathbb{Z}$, we omit the ring from the notation.

REMARK 3.3.29. We can also define full and cuspidal adjoint Hecke algebras $\mathfrak{H}_k^*(N, A)$ and $\mathfrak{h}_k^*(N, A)$. These are isomorphic as A-algebras to $\mathfrak{H}_k(N, A)$ and $\mathfrak{h}_k(N, A)$, respectively, via the map that takes a Hecke or diamond operator to its adjoint, which is well-defined for instance by the description of this map as conjugation by the Atkin-Lehner involution w_N. We write T^* for the adjoint of an operator T in $\mathfrak{H}_k(N, A)$ or $\mathfrak{h}_k(N, A)$

We shall also need a slight variation on $M_k(N, A)$.

DEFINITION 3.3.30. For a domain A with quotient field Q, we set

$$M_k'(N, A) = \{f \in M_k(N, Q) \mid a_n(f) \in A \text{ for all } n \geq 1\}.$$

EXAMPLE 3.3.31. For $k \geq 4$, the Eisenstein series E_k has integral coefficients aside from its constant term $-\frac{B_k}{2k}$, so lies in $M_k'(1, \mathbb{Z})$.

The Hecke algebra $\mathfrak{H}_k(N, A)$ acts on $M_k(N, Q)$ and preserves $M_k'(N, A)$. The following can be proven directly for $A = \mathbb{C}$, in some cases by construction of explicit bases of the spaces of modular forms, and then in general using the results of the next section.

THEOREM 3.3.32 (HIDA). *For any domain A, for each level N and weight $k \geq 2$, there is a perfect pairing*

$$M_k'(N, A) \times \mathfrak{H}_k(N, A) \to A, \qquad (f, T_n) \mapsto a_1(T_n f),$$

where $a_1(F)$ denotes the q-coefficient of a modular form F, and it induces a perfect pairing

$$S_k(N, A) \times \mathfrak{h}_k(N, A) \to A.$$

We may conclude from this the following.

PROPOSITION 3.3.33. *Let $f \in M_k(N, \chi)$ be an eigenform. The ring generated by the coefficients of f and the values of χ is an order in a number field K_f.*

PROOF. Note that $M_k(N, \mathbb{Z})$ is a finitely generated abelian group upon which $\mathfrak{H}_k(N)$ acts. The characteristic polynomial of any T_n acting on $M_k(N)$ is therefore monic with integral coefficients. In particular, if $f \in M_k(N, \chi)$ is an eigenform, then $a_n(f)$ is a root of this polynomial, so is an algebraic integer. The ring of coefficients is a quotient of $\mathfrak{H}_k(N, \mathbb{Z})$ via the homomorphism that sends T_n to $a_n(f)$ and $\langle j \rangle$ to $\chi(j)$. Being therefore an integral extension of $\mathbb{Z}$ of finite rank, we have the result. □

REMARK 3.3.34. The field K_f of an eigenform f as in Proposition 3.3.33 is generated over $\mathbb{Q}$ by its Fourier coefficients, as can be seen from (3.3.2).

3.4. Homology and cohomology

Until noted otherwise, we again treat $X_1(N)$ as a compact Riemann surface in this section. In fact, at first, we shall only need to think of its structure as a real manifold. That is, we first discuss its usual (i.e., singular, or "Betti") homology and cohomology.

First, note that we have an exact sequence of relative homology groups

$$0 \to H_1(X_1(N), \mathbb{Z}) \to H_1(X_1(N), C_1(N), \mathbb{Z}) \xrightarrow{\partial} \mathbb{Z}[C_1(N)] \to \mathbb{Z} \to 0, \tag{3.4.1}$$

where the latter two groups are 0th cohomology groups of $C_1(N)$ and $X_1(N)$, respectively.

REMARK 3.4.1. Pushforward by the action of $\delta_j \in \Gamma_0(N)$ on $X_1(N)$ gives rise to a diamond operator $\langle j \rangle = (\delta_j)_*$ on homology and cohomology groups. Similarly, we may define T_n via as a correspondence via $(\epsilon_n)_* \epsilon_1^*$, via pullback and pushforward by degeneracy maps, and we may define T_n^* as $(\epsilon_1)_* \epsilon_n^*$, as before. The sequence (3.4.1) is equivariant for these actions.

The definitions of homology and cohomology using dual complexes of singular chains and cochains give rise to perfect pairings

$$\begin{array}{ccc}
H_1(X_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & \xrightarrow{\cup} & \mathbb{Z} \\
\downarrow & & \| \\
H_1(X_1(N), C_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & & \| \\
\uparrow & & \| \\
H^1(X_1(N), C_1(N), \mathbb{Z}) \times H_c^1(Y_1(N), \mathbb{Z}) & \xrightarrow{\cup} & \mathbb{Z}
\end{array}$$

that are equivariant for the actions of Hecke operators.

We also have Poincaré duality, given by perfect cup product pairings

$$\begin{array}{ccccc}
H^1(X_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & \xrightarrow{\cup} & H^2(X_1(N), \mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z} \\
\downarrow & & & & \| \\
H^1(Y_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & & \downarrow \wr & & \| \\
\uparrow & & & & \| \\
H^1(Y_1(N), \mathbb{Z}) \times H_c^1(Y_1(N), \mathbb{Z}) & \xrightarrow{\cup} & H_c^2(Y_1(N), \mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z}.
\end{array}$$

where $H_c^i(Y_1(N), \mathbb{Z})$ denotes the ith compactly supported cohomology group. Hecke operators are adjoint to the adjoint operators under the cup product.

REMARK 3.4.2. More precisely, the definitions of homology and cohomology in terms of singular (co)chains, as well as Poincaré duality, give a Pontraygin duality between (co)homology with $\mathbb{Z}$-coefficients and compactly supported cohomology with $\mathbb{Q}/\mathbb{Z}$-coefficients (or vice versa for the coefficients). With $\mathbb{Z}$-coefficients on both sides, this can be reinterpreted as convergent spectral sequences

$$\mathrm{Ext}^i_{\mathbb{Z}}(H_j(X_1(N), C_1(N), \mathbb{Z}), \mathbb{Z}) \Rightarrow H_c^{i+j}(Y_1(N), \mathbb{Z})$$
$$\mathrm{Ext}^i_{\mathbb{Z}}(H^{2-j}(Y_1(N), \mathbb{Z}), \mathbb{Z}) \Rightarrow H_c^{i+j}(Y_1(N), \mathbb{Z})$$

and similarly with the groups reversed, or with taking instead the (co)homology of $X_1(N)$. Since all of our cohomology groups in question are free over $\mathbb{Z}$, the spectral sequences degenerate to give the above dualities.

Summarizing, we have a commutative diagram

$$\begin{array}{ccc} H_1(X_1(N),\mathbb{Z}) & \hookrightarrow & H_1(X_1(N),C_1(N),\mathbb{Z}) \\ \varphi\downarrow\wr & & \varphi\downarrow\wr \\ H^1(X_1(N),\mathbb{Z}) & \hookrightarrow & H^1(Y_1(N),\mathbb{Z}), \end{array}$$

where $\varphi(Tx) = T^*\varphi(x)$ for a Hecke (or diamond) operator T and its adjoint T^*.

REMARK 3.4.3. There is an involution τ on the homology and cohomology groups of modular curves induced by complex conjugation, which we can view as descended from the action $z \mapsto -\bar{z}$ on $\mathbb{H}^*$. Therefore, we can speak of plus and minus parts. The isomorphisms of Poincaré duality yield isomorphisms

$$H_1(X_1(N),C_1(N),\mathbb{Z})^{\pm} \xrightarrow{\sim} H^1(Y_1(N),\mathbb{Z})^{\mp}. \tag{3.4.2}$$

Next, let us compare with group (co)homology. Since $N \geq 4$, the group $\Gamma_1(N)$ contains no nontrivial elements of finite order, and it acts freely on the complexes of singular cochains for $\mathbb{H}$ with trivial coefficients (e.g., in $\mathbb{Z}$). It follows that we have a spectral sequence

$$H^i(\Gamma_1(N), H^j(\mathbb{H},\mathbb{Z})) \Rightarrow H^{i+j}(Y_1(N),\mathbb{Z}).$$

Since $\mathbb{H}$ is contractible, this quickly yields isomorphisms

$$H^i(\Gamma_1(N),\mathbb{Z}) \cong H^i(Y_1(N),\mathbb{Z}) \tag{3.4.3}$$

for all i, compatible with Hecke operators, which can be defined on the left by double cosets. The stabilizer $\Gamma_1(N)_x$ of a cusp x is the (infinite cyclic) intersection of a Borel subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with $\Gamma_1(N)$, and with the identification of (3.4.3), we have

$$H_1(X_1(N),\mathbb{Z}) \cong \ker\left(H_1(\Gamma_1(N),\mathbb{Z}) \to \bigoplus_{x\in C_1(N)} H_1(\Gamma_1(N)_x,\mathbb{Z}) \right).$$

DEFINITION 3.4.4. For $\alpha,\beta \in \mathbb{Q}\cup\{\infty\}$, the modular symbol $\{\alpha\to\beta\}_N$ is the class in the relative homology group $H_1(X_1(N),C_1(N),\mathbb{Z})$ of the geodesic from α to β in $\mathbb{H}^*$ (with respect to the hyperbolic metric $y^{-2}(dx^2+dy^2)$).

The boundary map ∂ of (3.4.1) satisfies

$$\partial(\{\alpha\to\beta\}) = \{\beta\} - \{\alpha\},$$

where for $x \in \mathbb{Q}\cup\{\infty\}$, the symbol $\{x\}$ denotes the class of x in the divisor group $\mathbb{Z}[C_1(N)]$. Since $\mathbb{H}$ is contractible, the modular symbols are independent of the chosen path with interior in $\mathbb{H}$, and they generate relative homology.

Cohomology with $\mathbb{C}$-coefficients has a decomposition into Hecke submodules via Hodge theory:

$$H^1(X_1(N),\mathbb{C}) \cong H^0(X_1(N),\Omega^1_{X_1(N)}) \oplus H^1(X_1(N),\mathcal{O}_{X_1(N)}). \tag{3.4.4}$$

Here, $\mathcal{O}_{X_1(N)}$ is the structure sheaf and $\Omega^1_{X_1(N)}$ is the sheaf of holomorphic differential 1-forms on $X_1(N)$. The summands are interchanged by complex conjugation, and they are isotropic under the cup product pairing of Poincaré duality. The Hecke module $H^0(X_1(N),\Omega^1_{X_1(N)})$ can be identified with $S_2(N)$ by viewing a weight 2 modular form f as the holomorphic differential on the curve induced by $2\pi i f(z)dz$. Hence $H^1(X_1(N),\mathcal{O}_{X_1(N)})$ can be identified with the antiholomorphic forms $\overline{S_1(N)}$. The group $H^1(Y_1(N),\mathbb{C})$ has a compatible decomposition to that of (3.4.4), where the second term is the same but the first is replaced by a sheaf of differentials with log poles at the cusps, and it is now isomorphic to $M_2(N)$. Consequently, we have the following.

Proposition 3.4.5. *The Hecke algebras generated by the diamond and Hecke operators inside the rings of endomorphisms of $H_1(X_1(N),\mathbb{Z})$ and $H_1(X_1(N),C_1(N),\mathbb{Z})$ are canonically isomorphic to the Hecke algebras $\mathfrak{h}_2(N)$ and $\mathfrak{H}_2(N)$.*

The decomposition (3.4.4) arises from the comparison of two cohomology theories: the Betti cohomology we have been considering, and de Rham cohomology. Rational structures on these isomorphic cohomology groups are compared by a period matrix with transcendental entries (see below).

The Betti and p-adic étale cohomology groups of modular curves with $\mathbb{Z}_p$-coefficients are also isomorphic, dependent upon a choice of embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Since $X_1(N)$ is smooth and proper over $\mathbb{Z}[\frac{1}{N}]$, the absolute Galois group of $\mathbb{Q}$ acts on its étale cohomology with $\mathbb{Z}_p$-coefficients (as well as the étale cohomology of $Y_1(N)$) via an action that is unramified outside of the primes dividing Np. It is the Galois action on étale cohomology we shall use in the next section. Poincaré duality provides an isomorphism between the Tate module of the Jacobian of $X_1(N)$ and $H^1_{\text{ét}}(X_1(N),\mathbb{Z}_p(1))$ that is both Galois equivariant and equivariant for the usual and adjoint Hecke actions on the respective sides.

We turn momentarily to modular symbols of higher weight. We may identify $\mathrm{Sym}^{k-2}\mathbb{Z}^2$ as the homogeneous, degree $k-2$ polynomials in two variables X and Y such that the (right) action of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ takes $P(X,Y)$ to $P(aX+bY, cX+dY)$. The following definition is somewhat convoluted due to potential issues of torsion.

Definition 3.4.6. For $\alpha,\beta \in \mathbb{Q}\cup\{\infty\}$ and $P \in \mathrm{Sym}^{k-2}\mathbb{Z}^2$, the weight k and level N modular symbol $P\{\alpha\to\beta\}$ is defined to be the class of $P\otimes\{\alpha\to\beta\}$ in

$$\mathrm{Sym}^{k-2}\mathbb{Z}^2 \otimes_{\mathbb{Z}[\Gamma_1(N)]} H_1(\mathbb{H}^*,\mathbb{P}^1(\mathbb{Q}),\mathbb{Z}).$$

The modular symbols $X^{i-1}Y^{k-i-1}\{\alpha\to\beta\}$ with $\alpha,\beta\in\mathbb{P}^1(\mathbb{Q})$ and $1\le i\le k-1$ span a lattice $\mathcal{M}_k(N,\mathbb{Z})$ called the group of weight k, level N modular symbols. The intersection of this lattice with the kernel of the boundary to $H_0(\mathbb{P}^1(\mathbb{Q}),\mathbb{Z})\otimes_{\mathbb{Z}[\Gamma_1(N)]}\mathrm{Sym}^{k-2}\mathbb{Z}^2$ is the subgroup $\mathcal{S}_k(N,\mathbb{Z})$ of cuspidal modular symbols. For any commutative ring R, we set $\mathcal{M}_k(N,R)=\mathcal{M}_k(N,\mathbb{Z})\otimes_{\mathbb{Z}}R$ and similarly for $\mathcal{S}_k(N,R)$.

Note that $\mathcal{M}_2(N,\mathbb{Z}) \cong H_1(X_1(N), C_1(N), \mathbb{Z})$ and $\mathcal{S}_2(N,\mathbb{Z}) \cong H_1(X_1(N),\mathbb{Z})$.

EXERCISE 3.4.7. Formulate Definition 3.4.6 in arbitrary weight $k \geq 2$ in terms of group cohomology, or relative homology.

EXERCISE 3.4.8. Formulate and prove the extension of Proposition 3.4.5 to arbitrary weight $k \geq 2$.

REMARK 3.4.9. The action of a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ with nonzero, positive determinant on a formal symbol $P\{\alpha \to \beta\}$ is given by

$$P\{\alpha \to \beta\} = (P\gamma^{-1})\{\gamma\alpha \to \gamma\beta\}.$$

This allows us to define Hecke operators on $\mathcal{M}_k(\mathbb{Z})$ as double coset operators.

A theorem of Eichler and Shimura [**Shi1**], as extended by Shokurov [**Sho1**] (see [**Mer**]), yields the following.

THEOREM 3.4.10. *We have an integration pairing of $\mathbb{C}$-vector spaces*

$$\langle\ ,\ \rangle \colon \mathcal{M}_k(N,\mathbb{C}) \times (S_k(N) \oplus \overline{S_k(N)}) \to \mathbb{C}$$
$$\langle P(X,Y)\{\alpha \to \beta\}, (f,g)\rangle = \int_\alpha^\beta f(z)P(z,1)dz + \int_\alpha^\beta f(z)P(\bar{z},1)d\bar{z},$$

where $P \in \mathbb{C}[X,Y]$ is homogeneous of degree $k-2$. This integration pairing is perfect upon restricting the first variable to elements of $\mathcal{S}_k(N,\mathbb{C})$, and the usual and adjoint operators are adjoint under this pairing.

EXERCISE 3.4.11. Compare this with Poincaré duality, for instance in weight 2 when the left-hand side is restricted to $H_1(X_1(N),\mathbb{C})$.

REMARK 3.4.12. The integration pairing of Theorem 3.4.10 provides the special values

$$L(f,j) = \frac{(-2\pi i)^j}{(j-1)!} r_j(f), \qquad r_j(f) = \langle X^{j-1}Y^{k-j-1}\{0 \to \infty\}, f\rangle.$$

of $f \in S_k(N)$ for $1 \leq j \leq k-1$.

EXERCISE 3.4.13. For a normalized eigenform $f \in S_k(N)$, there exist periods $\Omega_f^\pm$ such that the values of the pairing on classes in $\mathcal{M}_k(N,\mathbb{Q})^\pm$ all lie in $K_f\Omega_f^\pm$, where K_f is the field of coefficients of f.

EXERCISE 3.4.14. Show how to obtain special values of an appropriately defined L-function $L(f,\chi,s)$ for $f \in S_k(N)$ and a Dirichlet character χ of modulus dividing N via the integration pairing of Theorem 3.4.10.

EXAMPLE 3.4.15. Of particular interest to us are the L-values of weight k eigenforms at odd integers in the interior of the critical strip $[1, k-1]$. In weights k among 12, 16, 18, 20, 22, and

26, the spaces $S_k(1)$ are one-dimensional, and hence the unique normalized cusp form f_k in this space is already an eigenform, which is congruent to the Eisenstein series

$$E_k = -\frac{B_k}{4k} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n$$

at any prime p dividing the numerator of $\frac{B_k}{4k}$. Let us write out the table of these values $\frac{r_j(f_k)}{r_1(f_k)}$ for odd $3 \leq j \leq \frac{k-1}{2}$, for k up to 22. (It is reproduced from [**Man2**], after some rearranging, and the subscripts were a bit hard to read at points, so they could contain inaccuracies.)

k	$(\frac{r_3(f_k)}{r_1(f_k)}, \frac{r_5(f_k)}{r_1(f_k)}, \frac{r_7(f_k)}{r_1(f_k)}, \ldots)$
12	$\frac{691}{2^3 3^4 5 \cdot 7}(-2 \cdot 7, 3^2)$
16	$\frac{3617}{2^3 3^3 5 \cdot 7 \cdot 11 \cdot 13}(-2 \cdot 3 \cdot 11, 3 \cdot 7, -11)$
18	$\frac{43867}{2^6 3^3 5^4 7 \cdot 11 \cdot 13}(-2^2 \cdot 7 \cdot 11 \cdot 13, 3 \cdot 5^2 \cdot 11, -3^2 \cdot 13)$
20	$\frac{283 \cdot 617}{2^3 3^5 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}(-2 \cdot 3 \cdot 11 \cdot 13, 143, -3 \cdot 11, 2 \cdot 13)$
22	$\frac{131 \cdot 593}{2^5 3^3 5^4 7 \cdot 13 \cdot 17 \cdot 19}(-2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 17, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13, -2 \cdot 13 \cdot 17, 5 \cdot 17)$

The primes p such that $p \mid B_k$ appear in the numerators on the left of the right-hand columns. For each, we have a mod p congruence between $r_j(f_k)$ and the $r_j(E_k) = \frac{(j-1)!}{(-2\pi i)^j} L(E_k, j)$ for odd j with $3 \leq j \leq k-3$, the latter being zero by Example 3.3.7.

We end this section with the Manin-Drinfeld theorem.

THEOREM 3.4.16. *There exists a canonical, Hecke-equivariant splitting of the injection* $\mathcal{S}_k(N, \mathbb{Q}) \hookrightarrow \mathcal{M}_k(N, \mathbb{Q})$.

This was proven in weight 2 for $\Gamma_0(N)$ by use of the integration pairing of Theorem 3.4.10 and the operators $T_p - 1 - p$ for primes p not dividing N in a paper of Drinfeld [**Dri**], and the weight 2 analogue for $\Gamma_1(N)$ is proven by Manin in [**Man1**, Theorem 3.3]. In the general case, note that as the integration pairing is nondegenerate upon restriction to $\mathcal{S}_k(N, \mathbb{C})$, it immediately gives a $\mathbb{C}$-linear splitting of $\mathcal{S}_k(N, \mathbb{C}) \to \mathcal{M}_k(N, \mathbb{C})$. In [**Sho2**], Shokurov produces a basis in $\mathcal{M}_k(N, \mathbb{Z})$ of the left kernel of the pairing, which implies the theorem.

REMARK 3.4.17. The Manin-Drinfeld theorem is also a consequence of the Ramanujan-Petersson conjecture that $|a_p(f)| \leq 2p^{(k-1)/2}$ for all $p \nmid N$ (which Deligne showed follows from the Weil conjectures that he later proved). This says in particular that the Hecke eigenvalues of Eisenstein series and cuspidal eigenforms for primes p not dividing N are distinct.

3.5. Galois representations

Let $f \in S_k(N, \chi)$ be a newform, and fix a prime p. By a shift in notation, let $\mathcal{O}_f$ denote the valuation ring of the field K_f its coefficients generate over $\mathbb{Q}_p$, fixing an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$. Via the duality between cusp forms and the Hecke algebra, the normalized eigenform f gives rise to a ring homomorphism

$$\phi_f \colon \mathfrak{h}_k(N, \mathbb{Z}_p) \to \mathcal{O}_f$$

with $\phi_f(T_n) = a_n(f)$ and $\phi_f(\langle a \rangle) = \chi(a)$. Let $I_f = \ker \phi_f$.

REMARK 3.5.1. To give an idea of what the kernel I_f is, note that we may extend ϕ_f to a homomorphism $\mathcal{O}_f$-linearly to a map $\mathfrak{h}_k(N, \mathcal{O}_f) \to \mathcal{O}_f$, and the kernel of this map is generated by $T_n - a_n(f)$ for $n \geq 1$ and $\langle j \rangle - \chi(j)$ for all $j \in (\mathbb{Z}/N\mathbb{Z})^\times$.

The étale cohomology group

$$H^1(N) = H^1_{\text{ét}}(X_1(N)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)).$$

of the modular curve $X_1(N)$ over $\overline{\mathbb{Q}}$ is a Galois module that is unramified outside the primes dividing Np and which has a commuting Hecke action of adjoint Hecke operators.

REMARK 3.5.2. From now on, we use the convention that $T \in \mathfrak{H}_k(N, \mathbb{Z}_p)$ acts on cohomology through its adjoint T^*, so as to avoid speaking of adjoint operators below.

Suppose that $k = 2$. In this case, we set

$$V_f = H^1(N)/I_f H^1(N) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

which is a 2-dimensional K_f-vector space. This is isomorphic to the Galois representation attached to f by Shimura [**Shi1**].

DEFINITION 3.5.3. The p-adic Galois representation $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{K_f}(V_f)$ attached to f is the two-dimensional representation over K_f determined by the action of $G_{\mathbb{Q}}$ on V_f.

One typically fixes a choice of basis so that we can view ρ_f as a homomorphism $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f)$. A different choice yields a conjugate Galois representation.

THEOREM 3.5.4 (SHIMURA). *For any Frobenius φ_ℓ at a prime $\ell \nmid Np$, we have*

$$\det(\rho_f(\varphi_\ell)) = \ell\chi(\ell) \quad \textit{and} \quad \mathrm{Tr}(\rho_f(\varphi_\ell)) = a_\ell(f).$$

EXERCISE 3.5.5. The Galois representation ρ_f is characterized up to conjugacy by its trace and determinant on Frobenius elements φ_ℓ at primes $\ell \nmid Np$.

In [**Del**], Deligne constructed Galois representations ρ_f attached to newforms $f \in S_k(N, \chi)$ of arbitrary weight $k \geq 2$. For this, he takes the tensor product with $\mathbb{Q}_p$ of the quotient of an étale cohomology group by I_f, for instance of

$$H^1_{\text{ét}}(Y_1(N)_{/\overline{\mathbb{Q}}}, (\mathrm{Sym}^{k-2} \mathrm{Ta}_p \mathcal{E})(1)).$$

Here, $\mathrm{Ta}_p\mathcal{E}$ is the p-adic Tate module of the universal elliptic curve $\mathcal{E}_1(N)$, viewed as a sheaf over $X_1(N)_{/\bar{\mathbb{Q}}}$ (i.e., we take the first right-derived functor of the pushforward of $\mathbb{Z}_p(1)$). The trace of ρ_f on a Frobenius is again the corresponding Fourier coefficient, while $\det \rho_f = \chi_p^{k-1}\chi$.

REMARK 3.5.6. By the Manin-Drinfeld theorem, one obtains the same Galois representation from a modular form using cohomology of the open or closed curve, but not in general the same lattice (e.g., when f is p-adically congruent to an Eisenstein series).

CHAPTER 4

Hida theory and the main conjecture

4.1. Ordinary forms

Suppose in this section that N is divisible by p. For any prime ℓ dividing the level, the Hecke operator T_ℓ is frequently denoted U_ℓ, and we will also use this notation.

DEFINITION 4.1.1. A normalized eigenform f is said to be ordinary if $a_p(f) \in \mathcal{O}_f^\times$, i.e., is a p-adic unit.

Let $f \in S_k(N, \chi)$ be an ordinary newform. The property of being ordinary has important implications for the restriction of the Galois representation ρ_f to $G_{\mathbb{Q}_p}$, which is to say that it too is what is known as "ordinary", but as a Galois representation. In particular, there exists a basis of V_f with respect to which $\rho_f|_{G_{\mathbb{Q}_p}}$ is upper-triangular. On σ in the inertia subgroup I_p of $G_{\mathbb{Q}_p}$, it has the form

$$\rho_f(\sigma) = \begin{pmatrix} \chi_p\chi(\sigma) & * \\ 0 & 1 \end{pmatrix}.$$

Since we already know the determinant, another way of saying this is that V_f has a 1-dimensional inertia-fixed $G_{\mathbb{Q}_p}$-quotient.

Hida defined an idempotent of the Hecke algebra that projects to the "ordinary parts" of Hecke modules, which are the maximal submodules upon which U_p acts invertibly [**Hid1**].

PROPOSITION 4.1.2 (HIDA). *The element*

$$e^{\mathrm{ord}} = \lim_{n\to\infty} U_p^{n!}$$

is a well-defined idempotent of $\mathfrak{H}(N, \mathbb{Z}_p)$.

SKETCH OF PROOF. The $\mathbb{Z}_p$-algebra $\mathfrak{H}(N, \mathbb{Z}_p)$ is $\mathbb{Z}_p$-torsion free of finite rank, and as such, it is a product of complete noetherian local rings, each of which has semisimplification (i.e., quotient by nilradical) with quotient field a finite extension of $\mathbb{Q}_p$. Let u_p denote the projection of U_p to such a factor R. If u_p lies in the maximal ideal $\mathfrak{m}$ of R, then the limit of the $u_p^{n!}$ must approach 0. If, on the other hand, $u_p \in R^\times$, then $n!$ is divisible by the order of the residue field $R/\mathfrak{m}$ for sufficiently large n. Then $u_p^{n!} \equiv 1 \bmod \mathfrak{m}$, and as we further increase n, the quantity $n!$ becomes divisible by increasingly higher powers of p, which makes $u_p^{n!}$ congruent to 1 modulo increasing powers of $\mathfrak{m}$, forcing the limit of the $u_p^{n!}$ to be 1. Consequently, e^{ord} is an idempotent in $\mathfrak{H}(N, \mathbb{Q}_p)$. □

REMARK 4.1.3. The ring $e^{\mathrm{ord}}\mathfrak{H}(N, \mathbb{Z}_p)$ is a finite product of finite reduced $\mathbb{Z}_p$-algebras that are domains. The image of U_p in this ordinary Hecke algebra, which we also denote by U_p, is invertible.

DEFINITION 4.1.4. For an $\mathfrak{H}(N,\mathbb{Z}_p)$-module A, we define its ordinary part by $A^{\mathrm{ord}} = e^{\mathrm{ord}}A$.

REMARK 4.1.5. The perfect pairings between modular forms and Hecke algebras restrict to perfect pairings between their ordinary parts.

To indicate something of how we obtain the upper-triangular form of $\rho_f|_{G_{\mathbb{Q}_p}}$, we mention the following result that implies it. This result is a consequence of work of Mazur-Wiles, Tilouine, and Ohta (cf. [**Oht1**]) and is particularly suited for Hida theory.

THEOREM 4.1.6. *There is an exact sequence of $\mathfrak{h}_2(N,\mathbb{Z}_p)^{\mathrm{ord}}[G_{\mathbb{Q}_p}]$-modules*

$$0 \to H^1(N)^{\mathrm{ord}}_{\mathrm{sub}} \to H^1(N)^{\mathrm{ord}} \to H^1(N)^{\mathrm{ord}}_{\mathrm{quo}} \to 0,$$

that are free over $\mathbb{Z}_p$ and of rank one over $\mathfrak{h}_2(N,\mathbb{Z}_p)^{\mathrm{ord}}$, with $H^1(N)^{\mathrm{ord}}_{\mathrm{quo}}$ the maximal $\mathbb{Z}_p$-torsion-free quotient of $H^1(N)^{\mathrm{ord}}$ on which I_p acts trivially.

The theorem is proven by construction of an appropriate quotient the Jacobian $J_1(N)$ of $X_1(N)$ (typically) with good reduction at p. The application of Hida's idempotent to the ordinary part of the p-divisible group of its Neron model is of multiplicative type, and the injective image of its Tate module in the ordinary part of the Tate module $\mathrm{Ta}_p J_1(N)$ of $J_1(N)$ is dual under a twisted Weil pairing on $e^{\mathrm{ord}}\mathrm{Ta}_p J_1(N)$ to the resulting cokernel (on which I_p then acts trivially). The sequence is then the $\mathbb{Z}_p$-dual of the resulting exact sequence.

4.2. Hida theory

The ordinary parts of Hecke algebras, spaces of modular forms, and cohomology groups of modular curves (all with $\mathbb{Z}_p$-coefficients) have remarkable regularity properties as we increase the power of p that occurs in the level. In this way and others we shall soon see, Hida theory and Iwasawa theory have more than just superficial similarities. Contrary to the previous section, we now take N to be an integer prime to an odd prime p.

Hida theory deals with the behavior of modules over the ordinary part of the Hecke algebra as we increase r, i.e., the p-power in the level. Let $\mathcal{O}$ be the valuation ring of a finite extension of $\mathbb{Q}_p$, and set $\Lambda = \mathcal{O}[\![T]\!]$. We again identify Λ with $\mathcal{O}[\![1+p\mathbb{Z}_p]\!]$ by identifying T with $\gamma - 1$, where γ is the group element of our fixed topological generator υ. Recall that $Q(\Lambda)$ denotes the quotient field of Λ. We have a map $\kappa\colon \mathbb{Z}_p^\times \to \Lambda$ that is the projection to $1+p\mathbb{Z}_p$ followed by the map induced by the latter identification.

DEFINITION 4.2.1. A Λ-adic modular form of weight k, tame level N is a power series

$$f = \sum_{n=0}^{\infty} a_n(f) q^n \in Q(\Lambda) + q\Lambda[\![q]\!]$$

such that its specializations $f(\epsilon(\upsilon)\upsilon^{k-2}-1)$ at $T = \epsilon(\upsilon)\upsilon^{k-2}-1$ for a character $\epsilon\colon \Gamma \to \overline{\mathbb{Q}}_p^\times$ with kernel $\Gamma^{p^{r-1}}$ are modular forms of weight k, level Np^r, and character ϵ on the 1-units in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ for almost all such ϵ.

We may think of a Λ-adic modular form as a family of modular forms of varying (p-adic) weight.

DEFINITION 4.2.2. A Λ-adic modular form is a cusp form if all but finitely many of its specializations are cusp forms.

DEFINITION 4.2.3. We let $\mathfrak{M}'(N,\Lambda)$ and $\mathfrak{S}(N,\Lambda)$ denote the spaces of Λ-adic modular forms and Λ-adic cusp forms of weight 2 and tame level N, respectively. Let

$$\mathfrak{M}(N,\Lambda) = \mathfrak{M}'(N,\Lambda) \cap \Lambda[\![q]\!].$$

EXAMPLE 4.2.4. Let χ be an even $\mathcal{O}$-valued Dirichlet character of modulus Np. The Λ-adic Eisenstein series $\mathcal{E}_\chi \in \mathfrak{M}'(N,\Lambda)$ is

$$\mathcal{E}_\chi = \frac{1}{2}h_{\chi\omega^2} + \sum_{n=1}^{\infty}\sum_{\substack{d|n\\ p\nmid d}} \chi(d)(1+T)^{\log_\upsilon(d)}q^n,$$

where $h_{\chi\omega^2} \in Q(\Lambda)$ satisfies $h_{\chi\omega^2}(\upsilon^s - 1) = L_p(\chi\omega^2, -1-s)$ for $s \in \mathbb{Z}_p$ (with $h_{\chi\omega^2} \in \Lambda$ for $\chi\omega^2 \neq 1$), and where $\log_\upsilon(d)$ is taken to be the unique p-adic integer such that $\kappa(d) = \upsilon^{\log_\upsilon(d)}$. For all $k \geq 2$, we have $\mathcal{E}_\chi(\upsilon^{k-2} - 1) = E_{k,\chi\omega^{2-k}}$.

Set

$$\mathbb{Z}_{p,N} = \varprojlim_r \mathbb{Z}/Np^r\mathbb{Z}.$$

The nth Hecke operator for a prime n is then defined by the usual formula for its action on Fourier coefficients (see (3.3.2) for n prime). Each $j \in \mathbb{Z}_{p,N}^\times$ also yields a diamond operator $\langle j\rangle$ on $\mathfrak{M}(N,\Lambda)$, preserving the cusp forms, characterized by the property that it is compatible with the diamond operators on specializations. In particular, $\langle\upsilon\rangle$ acts as multiplication by $T+1$.

As before, we may define Hida's idempotent e^{ord} that acts on $\mathfrak{S}(N,\Lambda)$ and $\mathfrak{M}(N,\Lambda)$ and therefore the ordinary parts of the spaces of Λ-adic forms. Hida proved that these ordinary parts are free over Λ in [**Hid2**, Theorem 3.1] with a slightly different definition: the next result is found in Wiles [**Wil1**, Theorem 1.2.2]).

THEOREM 4.2.5 (HIDA, WILES). *The spaces $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ of ordinary Λ-adic forms are free of finite rank over Λ.*

We will concern ourselves here only with the well-behaved ordinary parts of Hecke algebras of Λ-adic forms.

DEFINITION 4.2.6. We let $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ denote the full modular and cuspidal ordinary Λ-adic Hecke algebras, which are the Λ-algebras generated by the Hecke and diamond operators inside the Λ-linear endomorphism rings of $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$, respectively.

Hida proved the following duality between ordinary modular forms and Hecke algebras [**Hid2**, Theorem 2.2].

THEOREM 4.2.7 (HIDA). *There is a perfect pairing of free, finite rank Λ-modules*

$$\mathfrak{M}'(N,\Lambda)^{\mathrm{ord}} \times \mathfrak{H}(N,\Lambda)^{\mathrm{ord}} \to \Lambda, \qquad (f, T_n) \mapsto a_1(T_n f),$$

that induces a perfect pairing

$$\mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \times \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \to \Lambda.$$

REMARK 4.2.8. It follows from Hida's duality theorem that $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ is a Cohen-Macaulay ring with dualizing module $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$, and $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ is Cohen-Macaulay with dualizing module $\mathfrak{M}'(N,\Lambda)^{\mathrm{ord}}$. If

$$\mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \cong \mathrm{Hom}_\Lambda(\mathfrak{h}(N,\Lambda)^{\mathrm{ord}},\Lambda)$$

is free over $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$, then $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ has the stronger property of being a Gorenstein ring. On the other hand, Wake showed that $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ are not always Gorenstein [**Wak**]. However, they become Gorenstein upon tensor product with $Q(\Lambda)$, and in particular $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ have rank one over their Hecke algebras.

For $r \geq 1$, let

$$\omega_{k,r} = (1+T)^{p^{r-1}} - \upsilon^{p^{r-1}(k-2)}.$$

The ordinary parts of the spaces of Λ-adic modular and cusp forms have a remarkable regularity, a sort of "perfect control" as the p-power in the level increases, whereby we can recover the spaces of ordinary forms of weight k and level Np^r simply by taking the quotient by $\omega_{k,r}$ [**Hid2**, Corollary 3.2].

THEOREM 4.2.9 (HIDA). *For all $r \geq 1$, we have*

$$\mathfrak{M}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong M_k(Np^r,\mathcal{O})^{\mathrm{ord}} \quad \text{and} \quad \mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong S_k(Np^r,\mathcal{O})^{\mathrm{ord}}$$

via isomorphisms that are equivariant with respect to the Hecke actions on both sides.

As a corollary, we have that ordinary Λ-adic forms and Hecke algebras are independent of the weight used, which explains our restriction to weight 2.

COROLLARY 4.2.10. *The spaces of ordinary Λ-adic modular forms of each weight $k \geq 2$ are all isomorphic via maps equivariant with respect to the corresponding ordinary Λ-adic Hecke algebras.*

REMARK 4.2.11. Note that under the identification of Λ with $\mathcal{O}[\![\Gamma]\!]$ for $\Gamma = 1 + p\mathbb{Z}_p$, the quotient of a Λ-module M by $\omega_{2,r}$ is equal to the $\Gamma^{p^{r-1}}$-coinvariant group of M, which is a $\mathcal{O}[\Gamma_r]$-module for $\Gamma_r = \Gamma/\Gamma^{p^{r-1}}$. One might compare this with the good control of p-parts of class groups described in our sketch of the proof of Theorem 2.3.12.

As a corollary of these two theorems, we obtain the following.

COROLLARY 4.2.12. *For all $r \geq 1$, we have*

$$\mathfrak{H}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathfrak{H}_k(Np^r,\mathcal{O})^{\mathrm{ord}} \quad \text{and} \quad \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathfrak{h}_k(Np^r,\mathcal{O})^{\mathrm{ord}}.$$

We have a similar regularity of ordinary parts of homology and cohomology groups of modular curves. That is, on homology, the canonical quotient maps on modular curves induce Hecke-equivariant surjections

$$H_1(X_1(Np^{r+1}),C_1(Np^{r+1}),\mathcal{O}) \to H_1(X_1(Np^r),C_1(Np^r),\mathcal{O})$$

which likewise induce (not necessarily surjective) maps on the first homology of the closed curves. On cohomology, the corresponding maps are the trace maps

$$H^1(Y_1(Np^{r+1}),\mathcal{O}) \to H^1(Y_1(Np^r),\mathcal{O})$$

that on the level of group cohomology correspond to corestriction. The latter maps are Hecke-equivariant for the dual action that we consider on cohomology. Again, we have perfect control of ordinary parts in the following sense [**Hid3**].

THEOREM 4.2.13 (HIDA). *The group* $\varprojlim_r H_1(X_1(Np^r),C_1(Np^r),\mathcal{O})^{\mathrm{ord}}$ *is free of finite rank over* Λ *and satisfies*

$$\left(\varprojlim_r H^1(X_1(Np^r),C_1(Np^r),\mathcal{O})^{\mathrm{ord}}\right)\otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathcal{M}_k(\mathcal{O})^{\mathrm{ord}}$$

as $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$*-modules. The analogous statement holds with usual homology and cuspidal modular symbols.*

Hida uses this theorem applied to étale cohomology in order to construct the Galois representations attached to ordinary Λ-adic cuspidal eigenforms. We can speak of such an eigenform as being a newform if its specializations, which are also eigenforms, are new at primes dividing N.

For a Λ-algebra $\mathcal{A}$, let us set $\mathfrak{S}(N,\mathcal{A}) = \mathfrak{S}(N,\Lambda)\otimes_\Lambda \mathcal{A}$. For a finitely generated profinite module $L = \varprojlim_\alpha L_\alpha$ over a complete commutative local ring A, we shall give $\mathrm{Aut}_A(L)$ the profinite topology as the inverse limit $\varprojlim_\alpha \mathrm{Aut}_A(L_\alpha)$ of finite groups. The following is the main theorem of [**Hid3**].

THEOREM 4.2.14 (HIDA). *Let* $\mathcal{F}\in\mathfrak{S}(N,\mathcal{A})^{\mathrm{ord}}$ *be a newform with character* χ *on* $(\mathbb{Z}/Np\mathbb{Z})^\times$*, where* $\mathcal{A}$ *is the integral closure of* Λ *in a finite extension* $\mathcal{Q}$ *of* $Q(\Lambda)$*. Then there exists a continuous Galois representation*

$$\rho_{\mathcal{F}}\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{A}}(\mathcal{L})$$

that is unramified outside of places dividing $Np\infty$*, where* $\mathcal{L}$ *is an* $\mathcal{A}$*-lattice in* $\mathcal{Q}^2$*, such that setting* $P_{k,\epsilon} = \epsilon(v)(1+T)^{k-2}-1$*, the resulting representation*

$$\rho_{\mathcal{F},k,\epsilon}\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{A}/(P_{k,\epsilon})}(\mathcal{L}/P_{k,\epsilon}\mathcal{L})$$

is isomorphic to the Galois representation attached to $f_{k,\epsilon} = \mathcal{F}(\epsilon(v)v^{k-2}-1)$*, for every* $k\geq 2$ *and continuous homomorphism* $\epsilon\colon 1+p\mathbb{Z}_p \to \overline{\mathbb{Q}}_p^\times$ *with finite image. This representation* $\rho_{\mathcal{F}}$ *has the property that*

$$\det(\rho_{\mathcal{F}}(\varphi_\ell)) = \ell\chi(\ell)(1+T)^{\log_v(\ell)} \quad\text{and}\quad \mathrm{Tr}(\rho_{\mathcal{F}}(\varphi_\ell)) = a_\ell(\mathcal{F})$$

for all primes $\ell\nmid Np$*, where* φ_ℓ *is an arithmetic Frobenius at* ℓ*.*

In fact, the construction proceeds in much the same way as the construction of Galois representations attached to a single form. That is, setting $\mathcal{O}=\mathbb{Z}_p$, we may consider

$$\mathcal{T}(N)^{\mathrm{ord}} = \varprojlim_r H^1(Np^r)^{\mathrm{ord}} = \varprojlim_r H^1_{\text{ét}}(X_1(Np^r),\mathbb{Z}_p(1))^{\mathrm{ord}},$$

with the inverse limit taken with respect to trace maps, which is of rank 2 over $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ (which is to say it is free of rank 2 over the total quotient ring) and free of finite rank over Λ. The lattice $\mathcal{L}$ can be taken to be $\mathcal{T}(N)^{\mathrm{ord}}/I_{\mathcal{F}}\mathcal{T}(N)^{\mathrm{ord}}$, where $I_{\mathcal{F}}$ is the kernel of the map $\phi_{\mathcal{F}}\colon \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \to \mathcal{A}$ taking T_n to $a_n(\mathcal{F})$ for $n \geq 1$.

The representation $\rho_{\mathcal{F}}$ is again upper-triangular with respect to a good choice of basis when restricted to $G_{\mathbb{Q}_p}$. This is a consequence of the following general result. We use $\mathfrak{h}^{\iota}$ to denote the Galois module on which an element of $G_{\mathbb{Q}}$ acts as $\langle \chi_p(\sigma)\rangle$, where χ_p is the p-adic cyclotomic character.

THEOREM 4.2.15 (OHTA, FUKAYA-KATO). *For $p \geq 5$, there is an exact sequence of $\mathfrak{h}^{\mathrm{ord}}[\![G_{\mathbb{Q}_p}]\!]$-modules*

$$0 \to \mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}} \to \mathcal{T}(N)^{\mathrm{ord}} \to \mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \to 0,$$

where $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}} \cong (\mathfrak{h}(N,\Lambda)^{\mathrm{ord}})^{\iota}(1)$ as $\mathfrak{h}[\![I_p]\!]$-modules, where I_p is the inertia subgroup of $G_{\mathbb{Q}_p}$. Here, $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}$ is the maximal Λ-torsion-free quotient of $\mathcal{T}(N)^{\mathrm{ord}}$ on which I_p acts trivially, and U_p acts as a Frobenius φ_p on $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}$.

In fact, what Ohta shows using p-adic Hodge theory is that there is a $G_{\mathbb{Q}_p}$-equivariant isomorphism

$$\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \hat{\otimes}_{\mathbb{Z}_p} R \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \hat{\otimes}_{\mathbb{Z}_p} R$$

after extending scalars from $\mathcal{O} = \mathbb{Z}_p$ to the completion R of the ring generated over $\mathbb{Z}_p$ by all roots of unity (cf. [**Oht1, Oht2**]). For this, Ohta identifies $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \hat{\otimes}_{\mathbb{Z}_p} R$ with an inverse limit over r of cotangent spaces of semistable quotients of the Jacobians of the curves $X_1(Np^r)$ constructed by Mazur-Wiles [**MaWi2**] and Tilouine [**Til**]. Fukaya and Kato point out in [**FuKa**, Proposition 1.7.9] that this descends to a canonical isomorphism

$$D(\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}) \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}},$$

where D is the functor given on compact $\mathfrak{h}[\![G_{\mathbb{Q}_p}]\!]$-modules T for a compact Λ-algebra $\mathfrak{h}$ by the submodule

$$D(T) = \{x \in T \hat{\otimes}_{\mathbb{Z}_p} W \mid (\varphi_p \otimes \varphi_p)(x) = x\}$$

of the completed tensor product, for W the completion of the integer ring of the maximal unramified extension of $\mathbb{Q}_p$ and φ_p the Frobenius map. The functor D is functorially but not canonically isomorphic to the forgetful functor from compact, unramified $\mathfrak{h}[\![G_{\mathbb{Q}_p}]\!]$-modules to compact $\mathfrak{h}$-modules, so $D(T) \cong T$ as $\mathfrak{h}$-modules. It is useful to note that this natural isomorphism is canonical upon restriction to the subcategory of modules with trivial $G_{\mathbb{Q}_p}$-action.

The result on $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}}$ is obtained by twisted Weil (or Poincaré) duality, which takes place through a perfect $\Lambda[G_{\mathbb{Q}}]$-equivariant pairing

$$\langle\ ,\ \rangle\colon \mathcal{T}(N)^{\mathrm{ord}} \times \mathcal{T}(N)^{\mathrm{ord}} \to \Lambda^{\iota}(1) \tag{4.2.1}$$

of Ohta's under which $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}}$ is its own annihilator [**Oht1**, Definition 4.1.17]. To obtain this pairing, one must modify the usual Poincaré duality pairing (using powers of U_p) to make it compatible with trace maps and by application of an Atkin-Lehner involution at each stage so that it has the property that $(Tx, y) = (x, Ty)$ for all $x, y \in \mathcal{T}(N)^{\mathrm{ord}}$ and $T \in \mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$.

4.3. Proof of the main conjecture

We now review the proof of the main conjecture in the spirit of Mazur-Wiles [**MaWi1**]. As in its statement, we restrict our discussion to fields of p-power roots of unity (so tame level $N = 1$), and let us suppose in our discussion that $p \geq 5$. We are only interested in irregular primes, so this restriction on p makes no difference to us. The approach we shall take is that of M. Ohta [**Oht2**].

Let us fix an even integer k.

DEFINITION 4.3.1. The Eisenstein ideal I_k of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ is the ideal generated by $U_p - 1$, the elements $T_\ell - 1 - \ell\langle\ell\rangle$ for all primes $\ell \neq p$, and $\langle j\rangle - \omega^{k-2}(j)$ for all $j \in \mu_{p-1}(\mathbb{Z}_p)$.

Consider the maximal ideal

$$\mathfrak{m}_k = I_k + (p, \langle \upsilon\rangle - 1)$$

containing I_k, where $\upsilon \in 1 + p\mathbb{Z}_p$ is as in (2.3.1). We can localize $\mathfrak{h}(1,\Lambda)$ at $\mathfrak{m}_k$, obtaining a local ring $\mathfrak{h}_k$ that is a direct factor of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$.

REMARK 4.3.2. We consider $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$, where $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ as a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \Lambda[\Delta]$-algebra for the inverses of diamond operators, where $\Delta = \mu_{p-1}(\mathbb{Z}_p)$. (This rather strange convention of taking inverse diamond operators will be convenient later.) As $\langle -1\rangle = 1$, the nontrivial eigenspaces of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ are all even. The algebra $\mathfrak{h}_k$ defined above is free of finite rank over Λ and by our convention has an ω^{2-k}-action of Δ.

For an even integer k, the algebra $\mathfrak{h}_k$ is nonzero if and only if $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ properly contains I_k. This in turn occurs if and only if the constant term $\frac{1}{2}h_{\omega^k}$ of the Λ-adic Eisenstein series $\mathcal{E}_{\omega^{k-2}}$ is not a unit, which is to say exactly when $p \mid B_{2,\omega^{k-2}}$. From now on, we suppose that this divisibility holds.

For simplicity of notation, we set $\mathfrak{h} = \mathfrak{h}_k$, we use $\mathcal{T}$ for $\mathcal{T}_{\mathfrak{m}_k}$, we use $\mathfrak{S}$ for $\mathfrak{S}(1,\Lambda)_{\mathfrak{m}_k}$, we use I for the image of I_k in $\mathfrak{h}$, and so on.

By a result of Manin and Drinfeld, the exact sequence

$$0 \to \mathfrak{S} \to \mathfrak{M} \to \Lambda \to 0 \tag{4.3.1}$$

is nearly split as a sequence of $\mathfrak{H}$-modules: that is, it splits if we first tensor the sequence over Λ with the quotient field $Q(\Lambda)$. Explicitly, this splitting takes $1 \in \Lambda$ to $\frac{2}{h_{\omega^k}}\mathcal{E}_k$. If s denotes this splitting and t denotes the corresponding splitting of $\mathfrak{S} \otimes_\Lambda Q(\Lambda) \to \mathfrak{M} \otimes_\Lambda Q(\Lambda)$, then the congruence module of the sequence (4.3.1) is defined to be

$$t(\mathfrak{M})/\mathfrak{S} \cong s(\Lambda)/(s(\Lambda) \cap \mathfrak{M}),$$

and it is isomorphic to $\Lambda/(\xi)$, where $\xi \in \Lambda$ satisfies $\xi(\upsilon^s - 1) = L_p(\omega^k, s-1)$ for $s \in \mathbb{Z}_p$. From this, we can conclude the following. The proof we give is due to Emerton [**Eme**].

THEOREM 4.3.3 (MAZUR-WILES). *We have an isomorphism $\mathfrak{h}/I \cong \Lambda/(\xi)$ of Λ-modules.*

PROOF. The Λ-adic Eisenstein series $\mathcal{E}_{\omega^{k-2}}$ has integral constant term since $k \not\equiv 0 \bmod p-1$, and one can show that every element of $\mathfrak{M}'$ does as well. By the duality of Hida, the modules $\mathfrak{M}$ and $\mathfrak{H}$ are Λ-dual to each other. In particular, $\mathcal{E}_{\omega^{k-2}}$ gives rise to a surjective homomorphism

$\mathfrak{H} \to \Lambda$ of Λ-algebras with kernel the Eisenstein ideal $\mathcal{I}$ in $\mathfrak{H}$. On the other hand, the surjection $\mathfrak{M} \to \Lambda$ that takes the involution ι applied to constant terms provides an element $T_0 \in \mathfrak{H}$ with kernel $\mathfrak{S}$ on $\mathfrak{M}$. The image of T_0 under $\mathfrak{H} \to \mathfrak{H}/I \cong \Lambda$ is then $\frac{1}{2}\xi$. We then have $\mathfrak{H}/(T_0) \cong \mathfrak{h}$, and if we take the quotient of both sides by the Eisenstein ideal (noting that I is the image of $\mathcal{I}$ in $\mathfrak{h}$), we obtain $\Lambda/(\xi)$. □

At p, we have an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules

$$0 \to \mathcal{T}_{\mathrm{sub}} \to \mathcal{T} \to \mathcal{T}_{\mathrm{quo}} \to 0, \tag{4.3.2}$$

This sequence is split as an exact sequence of $\mathfrak{h}$-modules. That is, by Theorem 4.2.15, the actions of $G_{\mathbb{Q}_p}$ on $\mathcal{T}_{\mathrm{sub}}$ and $\mathcal{T}_{\mathrm{quo}}$ factor through the maximal abelian quotient $G_{\mathbb{Q}_p}^{\mathrm{ab}}$. The unique order $p-1$ subgroup of its inertia group acts on $\mathcal{T}_{\mathrm{quo}}$ trivially and on $\mathcal{T}_{\mathrm{sub}}$ by ω^{k-1}, which is not the trivial character modulo p, allowing us to distinguish the two $\mathfrak{h}$-module summands.

Now, $\mathcal{T}_{\mathrm{sub}} \cong \mathfrak{h}$ and $\mathcal{T}_{\mathrm{quo}} \cong \mathfrak{S}$ as $\mathfrak{h}$-modules. Let $\mathcal{Q}$ denote the quotient field of $\mathfrak{h}$, and note that $V_- = \mathcal{T}_{\mathrm{sub}} \otimes_{\mathfrak{h}} \mathcal{Q}$ and $V_+ = \mathcal{T}_{\mathrm{quo}} \otimes_{\mathfrak{h}} \mathcal{Q}$ are 1-dimensional subspaces of $V = \mathcal{T} \otimes_{\mathfrak{h}} \mathcal{Q}$. Let us fix an ordered basis of V consisting of an element of V_- and an element of V_+, in that order, yielding a p-ramified representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{Q}), \qquad \rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

which is upper-triangular on $G_{\mathbb{Q}_p}$ and for $\tau \in I_p$ has the form

$$\rho(\tau) = \begin{pmatrix} \chi_p(\tau)\langle\chi_p(\tau)\rangle & b(\tau) \\ 0 & 1 \end{pmatrix}.$$

Both $a(\sigma)$ and $d(\sigma)$ lie in $\mathfrak{h}$ inside $Q(\mathfrak{h})$: for this, note that $\mathrm{Hom}_{\mathfrak{h}}(\mathfrak{S}, \mathfrak{S}) \cong \mathfrak{h}$. Since $\det \rho(\sigma) \in \mathfrak{h}$ as well, we also have $b(\sigma)c(\sigma) \in \mathfrak{h}$. In fact, we have the following lemma of Kurihara and Harder-Pink, which was applied to the Λ-adic setting by Ohta.

LEMMA 4.3.4. *The elements $a(\sigma) - \det \rho(\sigma)$, $d(\sigma) - 1$, and $b(\sigma)c(\tau)$ are contained in I for all $\sigma, \tau \in G_{\mathbb{Q}}$.*

PROOF. By plugging 1 into the characteristic polynomial for (the adjoint action of) the ℓth Hecke operator, which is also that of the Frobenius φ_ℓ for $\ell \neq p$, we have

$$1 - (a(\varphi_\ell) + d(\varphi_\ell)) + \det \rho(\varphi_\ell) = 1 - T_\ell + \ell\langle\ell\rangle \in I$$

By the Čebotarev density theorem, the φ_ℓ are dense in $G_{\mathbb{Q}}$, so by continuity of our Galois representation, we have

$$1 - a(\sigma) - d(\sigma) + \det \rho(\sigma) \in I \tag{4.3.3}$$

for all $\sigma \in G_{\mathbb{Q}}$. Let $\theta \in I_p$ restrict to $-1 \in \mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. By construction, we have $\rho(\theta) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so replacing σ with $\theta\sigma$ in (4.3.3), we obtain

$$1 + a(\sigma) - d(\sigma) - \det \rho(\sigma) \in I$$

and taking the sum and difference of the two equations gives us the first two containments. We then need only note that

$$c(\tau)b(\sigma) = (d(\tau\sigma) - 1) - (d(\tau)d(\sigma) - 1) \in I.$$

□

Now, let B and C denote the $\mathfrak{h}$-spans in $Q(\mathfrak{h})$ of the images of b and c, respectively. Then $BC \subseteq I$ is an ideal of $\mathfrak{h}$ independent of the choice of basis that we made. Another application of Cebotarev density shows that a positive density of Frobenius elements satisfy $d(\varphi_\ell) - 1 \in BC$, which implies that a similar positive density of elements $T_\ell - 1 - \ell\langle\ell\rangle$ lie in BC. From this, we may conclude that BC is a faithful $\mathfrak{h}$-module, and therefore B and C are as well.

Now, let us consider the map

$$\psi_c \colon G_{\mathbb{Q}} \to C/IC, \qquad \psi_c(\sigma) = (\det \rho(\sigma))^{-1} c(\sigma) + IC.$$

This is a cocycle, as matrix multiplication provides the equality

$$c(\sigma\tau) = \det(\rho(\tau))c(\sigma) + c(\tau)d(\tau)$$

for all $\sigma, \tau \in G_{\mathbb{Q}}$, and $d(\tau) - 1 \in I$. Moreover, the restriction of ψ_c to F_∞ is clearly a homomorphism, and by definition it is unramified at p, hence everywhere. Also, for any $\sigma \in G_{\mathbb{Q}}$ and $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$, we have

$$\psi_c(\sigma\tau\sigma^{-1}) = \det \rho(\sigma)^{-1}\psi_c(\tau) = \omega^{1-k}(\sigma)\kappa(\sigma)^{-1}\langle\kappa(\sigma)\rangle^{-1}\psi_c(\tau) = \chi_p(\sigma)^{-1}\sigma\psi_c(\tau)$$

Thus the restriction of ψ_c factors through $X_\infty^{(1-k)}$, and if we twist the source by $\mathbb{Z}_p(1)$, the resulting map

$$\bar{c} \colon X_\infty^{(1-k)}(1) \to C/IC$$

is a homomorphism of Λ-modules for the Λ-module structures arising from the Galois actions on both sides. On C/IC, this Λ-module structure agrees with that coming from the action of inverses of diamond operators.

By construction, the span of the image of ψ_c is C/IC. By considering the images of commutators with the element θ considered in the proof of Lemma 4.3.4, one may check that $\bar{c}$ is itself surjective. The surjectivity of $\bar{c}$ tells us that the characteristic ideal of $X_\infty^{(1-k)}(1)$ is divisible by the characteristic ideal of C/IC. Since C is a faithful $\mathfrak{h}$-module, one can use the theory of Fitting ideals to show that the Eisenstein quotient C/IC has characteristic ideal divisible by the characteristic ideal of $\mathfrak{h}/I$, which is of course (ξ). For the element f_k that appears in the main conjecture, we have $f_k(v^s - 1) = \xi(v^{s+1} - 1)$. Thus, we may conclude that $f_k \mid \mathrm{char}(X_\infty^{(1-k)})$ for all k, which implies equality by the analytic class number formula, as noted in Remark 2.5.2.

4.4. The map Υ

We continue with the notation of the previous section. We will view $\overline{\mathbb{Q}}$ as the algebraic numbers in $\mathbb{C}$, which fixes in particular a complex conjugation, a generator of the Tate module $\mathbb{Z}_p(1)$, and isomorphisms between Betti and étale cohomology groups of modular curves.

In the proof of the main conjecture, we in essence used the $\mathfrak{h}$-lattice in $\mathcal{T} \otimes_{\mathfrak{h}} \mathcal{Q}$ that is given by the $\mathfrak{h}[G_{\mathbb{Q}}]$-module span of $\mathcal{T}_{\mathrm{sub}}$. This has the form $\mathcal{T}_{\mathrm{sub}} \oplus C'$, for $C' \subset \mathcal{T}_{\mathrm{quo}} \otimes_{\mathfrak{h}} \mathcal{Q}$, where C is identified with $\mathrm{Hom}_{\mathfrak{h}}(\mathcal{T}_{\mathrm{sub}}, C')$. By choosing this lattice, we insure that the homomorphism $\bar{c}$ is surjective. This may seem rather unnatural, and from our perspective it is. Therefore, in this section, we construct a related map Υ using the lattice $\mathcal{T}$ arising from the homology of the closed modular curves, as first defined in [**Sha3**].

We shall play two decompositions of $\mathcal{T}$ into rank one $\mathfrak{h}$-module summands off of each other. These each arise by looking locally at a place of $\mathbb{Q}$: that corresponding to p which we have already discussed and the decomposition $\mathcal{T} = \mathcal{T}^+ \oplus \mathcal{T}^-$ corresponding to the real place. We view $\mathcal{T}/\mathcal{T}^+$ as $\mathcal{T}^-$ in what follows. Set

$$\mathcal{S} = \varprojlim_r H_1(X_1(p^r), \mathbb{Z}_p)^+_{\mathfrak{m}_k},$$

which is isomorphic by our choice of complex embedding to $\mathcal{T}^+$. Our goal is to show that $\mathcal{T}^+/I\mathcal{T}^+$ is both $G_{\mathbb{Q}}$-stable in and a $G_{\mathbb{Q}_p}$-summand of $\mathcal{T}/I\mathcal{T}$, so that we have an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}}]$-modules

$$0 \to \mathcal{T}^+/I\mathcal{T}^+ \to \mathcal{T}/I\mathcal{T} \to \mathcal{T}^-/I\mathcal{T}^- \to 0 \tag{4.4.1}$$

that is canonically locally split at p. Moreover, we claim that $\mathcal{T}^-/I\mathcal{T}^-$ is free of rank 1 over $\mathfrak{h}/I$ with a canonical generator z. Given these facts, we define a homomorphism

$$\Upsilon\colon X^{(1-k)}(1) \to \mathcal{S}/I\mathcal{S}$$

as the composition of the restriction of the 1-cocycle $G_{\mathbb{Q}} \to \mathrm{Hom}_{\mathfrak{h}}(\mathcal{T}^-/I\mathcal{T}^-, \mathcal{T}^+/I\mathcal{T}^+)$ defined by (4.4.1) with evaluation at z. Explicitly, if $q\colon \mathcal{T}/I\mathcal{T} \to \mathcal{T}^-/I\mathcal{T}^-$ denotes the projection, then the cocycle is given on $x \in \mathcal{T}^-/I\mathcal{T}^- \subset \mathcal{T}/I\mathcal{T}$ by

$$x \mapsto \sigma(q(\sigma^{-1}x)) - x.$$

Since $G_{\mathbb{Q}}$ acts nontrivially on $\mathcal{T}^-/I\mathcal{T}^-$, the continuous homomorphism Υ is not $G_{\mathbb{Q}}$-equivariant, but it is still a map of $\Lambda[\Delta]$-modules if we take the Galois action of $\mathbb{Z}_p^\times$ on the left and the action of inverse diamond operators in $\mathbb{Z}_p^\times$ on the right.

Lemma 4.4.1. *The $\mathfrak{h}[G_{\mathbb{Q}}]$-module $Z = \mathcal{T}/I\mathcal{T}$ has a quotient Q canonically isomorphic to $(\Lambda/(\xi))^\iota(1)$.*

Proof. We consider the inverse limit

$$\tilde{\mathcal{T}} = \varprojlim_r H^1_{\text{ét}}(Y_1(p^r), \mathbb{Z}_p(1))_{\mathfrak{m}_k}$$

of the Eisenstein part of cohomology groups of the open modular curves of increasing p-power level. This $\mathfrak{H}$-module $\tilde{\mathcal{T}}$ has the properties that $\tilde{\mathcal{T}}_{\mathrm{sub}} = \mathcal{T}_{\mathrm{sub}}$, while $\tilde{\mathcal{T}}/\mathcal{T} \cong \Lambda$ is generated as a Λ-module by image of the compatible sequence of modular symbols $\{0 \to \infty\}$ at levels p^r. By Theorem 4.2.15 and its analogue for $\tilde{\mathcal{T}}$, we also have $\tilde{\mathcal{T}}/\mathcal{T} \cong \mathfrak{M}/\mathfrak{S}$.

Recall that we have a splitting $t\colon \mathfrak{M} \to \mathfrak{S} \otimes_\Lambda Q(\Lambda)$ of $\mathfrak{H} \otimes_\Lambda Q(\Lambda)$-modules. This induces a splitting $\tilde{\mathcal{T}}_{\mathrm{quo}} \to \mathcal{T}_{\mathrm{quo}} \otimes_\Lambda Q(\Lambda)$ and therefore a splitting $t\colon \tilde{\mathcal{T}} \to \mathcal{T} \otimes_\Lambda Q(\Lambda)$ (via our splitting of $\mathcal{T} \to \mathcal{T}_{\mathrm{quo}}$ and the compatible splitting for $\tilde{\mathcal{T}}$). We then have an isomorphism $t(\tilde{\mathcal{T}})/\mathcal{T} \cong \Lambda/(\xi)$

sending the image of $\{0 \to \infty\}$ to 1. In particular, we have that $x = \xi t(\{0 \to \infty\})$ is part of a Λ-basis of $\mathcal{T}$, and the Λ-module homomorphism

$$\pi\colon \mathcal{T} \to \Lambda, \qquad \pi(a) = \langle x, a \rangle$$

given by Ohta's pairing (4.2.1) is surjective. Note that $t(\tilde{\mathcal{T}})/\mathcal{T}$ is a Galois module upon which $G_{\mathbb{Q}}$ acts trivially. The image of x in Z is then also fixed by $G_{\mathbb{Q}}$, so lies in Z^+. By the Galois equivariance of Ohta's pairing $\mathcal{T} \times \mathcal{T} \to \Lambda^\iota(1)$, the map π induces a surjection of $\Lambda[G_{\mathbb{Q}}]$-modules $\bar{\pi}\colon Z^- \to Q$ for $Q = (\Lambda/(\xi))^\iota(1)$. □

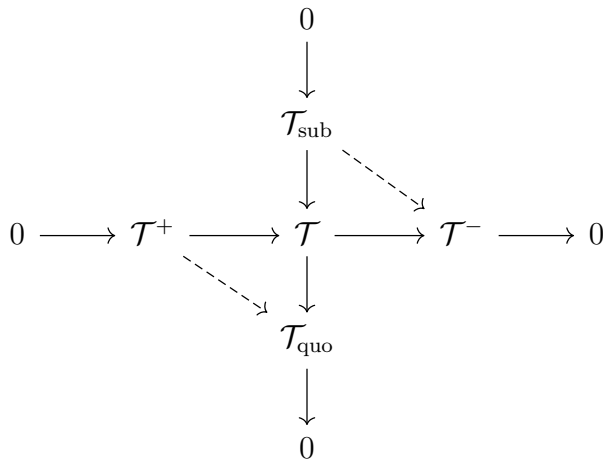
Let $P = \ker(Z \to Q)$, so we have a global exact sequence

$$0 \to P \to Z \to Q \to 0. \tag{4.4.2}$$

The second half of the following proposition now implies that this sequence agrees with (4.4.1) and is locally split, allowing us to construct Υ in the manner already described above.

Proposition 4.4.2 (Fukaya-Kato). *The composite maps $\mathcal{T}^+ \to \mathcal{T} \to \mathcal{T}_{\mathrm{quo}}$ and $\mathcal{T}_{\mathrm{sub}} \to \mathcal{T} \to \mathcal{T}^-$ are isomorphisms. Moreover, $P = Z^+$, the $\mathfrak{h}/I$-module Z^- is free with a canonical generator, and* (4.4.2) *is canonically split as an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules.*

That is, we have a commutative diagram



where the diagonal arrows are isomorphisms.

Proof. The first isomorphism follows from the second. For the second, since $\mathcal{T}_{\mathrm{sub}} \cong \mathfrak{h}$ and $\mathcal{T}^-$ has $\mathfrak{h}$-rank 1, it suffices to verify the surjectivity of $\mathcal{T}_{\mathrm{sub}} \to \mathcal{T}^-$. By Nakayama's lemma, this is further reduced to the surjectivity of $\mathcal{T}_{\mathrm{sub}} \to Z^-$.

Set $Z_{\mathrm{sub}} = \mathcal{T}_{\mathrm{sub}}/I\mathcal{T}_{\mathrm{sub}}$ and $Z_{\mathrm{quo}} = \mathcal{T}_{\mathrm{quo}}/I\mathcal{T}_{\mathrm{quo}}$. We claim that the composite map $Z_{\mathrm{sub}} \to Z \to Q$ of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules is an isomorphism. Since both the source and target are free of rank 1 over $\mathfrak{h}/I$, it suffices to show surjectivity. The cokernel is isomorphic to an $\mathfrak{h}[G_{\mathbb{Q}_p}]$-module quotient of Z_{quo}, but every lift of an element of $\Delta \cong \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ to I_p fixes Z_{quo} but no nonzero element of Q, proving the claim.

Since $Z_{\mathrm{sub}} \to Q$ is an isomorphism, $P \to Z_{\mathrm{quo}}$ is an isomorphism as well. The global exact sequence (4.4.2) is therefore locally split at p by the composite map $Z \to Z_{\mathrm{quo}} \xrightarrow{\sim} P$, as claimed.

It remains, then, only to verify that $P = Z^+$, as this implies that the surjection $Z^- \to Q$ is an isomorphism with a canonical generator z satisfying $\bar{\pi}(z) = 1$. Since $d(\sigma) - 1 \in I$ for all $\sigma \in G_{\mathbb{Q}}$, any complex conjugation acts trivially on Z_{quo}. In other words, P is contained in, and hence equal to, Z^+ inside Z. □

REMARK 4.4.3. Note that $Z^+ \cong \mathcal{S}/I\mathcal{S}$ as Λ-modules as well, as Frobenius acts as U_p on $\mathcal{T}_{\mathrm{quo}}$ (see [**FuKa**, Prop. 1.8.1]), hence trivially on Z_{quo}.

CHAPTER 5

Modular symbols and arithmetic

5.1. Galois cohomology and cup products

We begin this chapter by delving a bit deeper into our study of the arithmetic of cyclotomic fields. For this, we first review some Galois cohomology, which is already quite useful in what we have summarized above. Let K be a number field, and let p be a prime. We suppose that p is odd or K has no real places. We fix a finite set S of finite places of K that contains all places dividing primes over p.

DEFINITION 5.1.1. We use $G_{K,S}$ to denote the Galois group of the maximal S-ramified (or in more usual terminology, unramified outside S and any real places) extension Ω of K.

Let us use A to denote a discrete $\mathbb{Z}[G_{K,S}]$-module. We consider the Galois cohomology groups $H^i(G_{K,S}, A)$ defined by continuous cochains.

REMARK 5.1.2. The group $G_{K,S}$ is a finitely topologically generated profinite group of cohomological dimension 2. That is, the profinite cohomology groups $H^i(G_{K,S}, A)$ are trivial for $i \geq 3$.

REMARK 5.1.3. If K is Galois over some subfield E and A is a discrete $\mathbb{Z}[\mathrm{Gal}(\Omega/E)]$-module, then $\mathrm{Gal}(K/E)$ acts on the groups $H^i(G_{K,S}, A)$. That is, we let $\sigma \in \mathrm{Gal}(K/E)$ act on an inhomogenous i-cochain $f\colon G^i \to A$ by

$$(\sigma \cdot f)(g) = \tilde{\sigma} f(\tilde{\sigma}^{-1} g \tilde{\sigma})$$

for $g \in G_{K,S}^i$ and $\tilde{\sigma} \in \mathrm{Gal}(\Omega/E)$, and this induces an action on cohomology independent of the choice of lift.

Of particular interest is the case of μ_{p^n}-coefficients, for which the following objects are useful.

DEFINITION 5.1.4.

- Let $\mathcal{O}_{K,S}$ denote the ring of S-integers of K, i.e., elements of K which can be expressed as quotients of elements in $\mathcal{O}_K$ with denominators divisible only by primes in S.
- Let $\mathcal{E}_{K,S} = \mathcal{O}_{K,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ denote the p-completion of the group of S-units of K.
- Let $\mathrm{Cl}_{K,S}$ denote the S-class group of K, i.e., the quotient of the class group Cl_K by the classes of the primes in S, or alternatively, the class group of $\mathcal{O}_{K,S}$.

PROPOSITION 5.1.5. *For all $n \geq 1$, we have canonical exact sequences*

$$0 \to \mathcal{E}_{K,S}/\mathcal{E}_{K,S}^{p^n} \to H^1(G_{K,S}, \mu_{p^n}) \to \mathrm{Cl}_{K,S}[p^n] \to 0$$

$$0 \to \mathrm{Cl}_{K,S}/p^n\mathrm{Cl}_{K,S} \to H^2(G_{K,S}, \mu_{p^n}) \to \textstyle\bigoplus_{v \in S} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sum} \mathbb{Z}/p^n\mathbb{Z} \to 0.$$

The first of these sequences can be derived by Kummer theory, just as in the derivation of (2.3.3). In fact, $H^1(G_{K,S}, \mu_{p^n})$ is the quotient by $K^{\times p^n}$ of the subgroup $\mathcal{B}_{n,K,S}$ of $K^\times$ consisting of those elements a such that the fractional ideal $a\mathcal{O}_{K,S}$ is a p^nth power. The second employs Kummer theory and/or the Poitou-Tate sequence, which we shall not review here, but see [**NSW**, Chapter 8].

REMARK 5.1.6. If K is Galois over E, then the exact sequences of Proposition 5.1.5 are of $\mathbb{Z}_p[\mathrm{Gal}(K/E)]$-modules.

EXAMPLE 5.1.7. Set $F_r = \mathbb{Q}(\mu_{p^r})$ for $r \geq 1$, and let S denote the set of its primes over p. Then S consists of the single principal ideal $(1 - \zeta_{p^r})$, so $\mathrm{Cl}_{F_r,S} \cong \mathrm{Cl}_{F_r}$, and for $n \geq 1$, we have isomorphisms

$$H^2(G_{F_r,S}, \mu_{p^n}) \cong A_r/p^n A_r,$$

where $A_r = \mathrm{Cl}_{F_r} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as before.

We are particularly interested in the cup products

$$H^1(G_{K,S}, \mu_{p^n}) \otimes H^1(G_{K,S}, \mu_{p^n}) \xrightarrow{\cup} H^2(G_{K,S}, \mu_{p^n}^{\otimes 2})$$

If $\mu_{p^n} \subset K$, then the Galois action on $\mu_{p^n}^{\otimes 2}$ is trivial, so as modules over $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$, we have

$$H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}) \cong H^2(G_{K,S}, \mu_{p^n}) \otimes_{\mathbb{Z}_p} \mu_{p^n},$$

allowing us to use the description of $H^2(G_{K,S}, \mu_{p^n})$ in (5.1.5). These cup products induce pairings

$$(\ ,\ )_{p^n,K,S} \colon \mathcal{B}_{n,K,S} \times \mathcal{B}_{n,K,S} \to H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}),$$

which again are $\mathrm{Gal}(K/E)$-equivariant if K is Galois over a subfield E. Composition with the restriction map

$$H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}) \to H^2(G_{K_v}, \mu_{p^n}^{\otimes 2}) \xrightarrow{\sim} \mu_{p^n},$$

where K_v is the completion of K at v and the latter map is the invariant map of class field theory, is the restriction of the Hilbert norm residue symbol

$$(\ ,\ )_{p^n,K_v} \colon K_v^\times \times K_v^\times \to \mu_{p^n}.$$

McCallum and the author proved the following formula for this pairing [**McSh**].

THEOREM 5.1.8 (MCCALLUM-S.). *Suppose that $\mu_{p^n} \subset K^\times$, and let $a, b \in \mathcal{O}_{K,S}^\times$ be such that the norm residue symbols $(a,b)_{p^n,K_v}$ vanish for all $v \in S$. Let α be an p^nth root of a, let $L = K(\alpha)$, and let $G = \mathrm{Gal}(L/K)$. We may write $b = N_{L/K}y$ for some $y \in L^\times$ and $y\mathcal{O}_{L,S} = \mathfrak{c}^{1-\sigma}$ with $\mathfrak{c}$ an ideal of $\mathcal{O}_{L,S}$ and $\sigma \in G$. Then*

$$(a,b)_{p^n,K,S} = N_{L/K}\mathfrak{c} \otimes \alpha^{\sigma-1} \in \mathrm{Cl}_{K,S} \otimes_{\mathbb{Z}} \mu_{p^n}.$$

COROLLARY 5.1.9. *If $a, 1-a \in \mathcal{O}_{K,S}^\times$, then $(a, 1-a)_{p^n,K,S} = 0$.*

PROOF. In the notation of the theorem, we have $1 - a = N_{L/K}(1-\alpha)$, and $1 - \alpha \in \mathcal{O}_{L,S}^\times$. □

Again take $F_n = \mathbb{Q}(\mu_{p^n})$, with S the set of primes over p. In this case, we restrict our cup product to the cyclotomic p-units and then extend it to the p-completion $\mathcal{C}_n$ to yield an antisymmetric, $\mathrm{Gal}(F_n/\mathbb{Q})$-equivariant, bilinear pairing

$$(\ ,\ )_n \colon \mathcal{C}_n \times \mathcal{C}_n \to A_n \otimes_{\mathbb{Z}} \mu_{p^n}.$$

By Corollary 5.1.9 and the fact that $\mathcal{C}_n \cong \mathcal{C}_n^+ \oplus \mu_{p^n}$, we have $(\zeta_{p^n}, 1-\zeta_{p^n}^i)_{p^n,F_n,S} = 0$ for all $1 \leq i < p^n$, so our pairing factors through $\mathcal{C}_n^+$ in each variable and therefore lands in $(A_n \otimes_{\mathbb{Z}} \mu_{p^n})^+ \cong A_n^- \otimes \mu_{p^n}$.

Remark 5.1.10. From Corollary 5.1.9, one can already find a number of interesting pairs on which the pairing vanishes. For instance, we have

$$\frac{1-x^a}{1-x^{a+b}} + x^a \frac{1-x^b}{1-x^{a+b}} = 1 \tag{5.1.1}$$

$$\frac{(1-x^{2a})(1-x^{a+b})}{(1-x^a)(1-x^{2(a+b)})} - x^a \frac{(1-x^b)(1-x^{a+b})}{1-x^{2(a+b)}} = 1 \tag{5.1.2}$$

$$x^b \frac{(1-x^{3a})(1-x^{a+b})}{(1-x^a)(1-x^{3(a+b)})} + \frac{(1-x^b)(1-x^{a+b})(1-x^{2a+b})}{1-x^{3(a+b)}} = 1 \tag{5.1.3}$$

for $a, b \geq 1$, which we can apply to $x = \zeta_{p^n}$ (with appropriate conditions on a and b).

Consider $n = 1$. The eigenspaces $\mathcal{C}_1^{(1-i)}$ for i odd are isomorphic to $\mathbb{Z}_p$, generated by elements η_i that are the projections of $1-\zeta_p$ to these spaces. For any even k, set

$$e_{i,k} = (\eta_i, \eta_{k-i})_1 \in A^{(1-k)} \otimes_{\mathbb{Z}} \mu_p,$$

where $A = A_1$. Note that the eigenspaces here match up as $A^{(1-k)} \otimes_{\mathbb{Z}} \mu_p \cong (A \otimes_{\mathbb{Z}} \mu_p)^{(2-k)}$. These elements $e_{i,k}$ generate the span of the image of the pairing.

Note that if $p \mid B_k$, then in all known cases, $A^{(1-k)} \cong \mathbb{F}_p$ as a group, which is to say for $p < 39 \cdot 2^{22}$ [**BuHa**]. In these cases, one might think of the values $e_{i,k}$ as i varies as lying in $\mathbb{F}_p$ via a choice of generator. Via a computation, we showed in [**McSh**] that for $p < 25000$ and k with $p \mid B_k$, there exists up to scalar a unique nontrivial, antisymmetric, Galois-equivariant pairing $\mathcal{C}_1 \times \mathcal{C}_1 \to \mathbb{F}_p(2-k)$ that satisfies the relations (5.1.2) in Remark 5.1.10.

Example 5.1.11. Here is a table of the relative values of the $e_{i,k}$, normalized so that $e_{1,k} = 1$. (From what we have said, it is not clear that these values are nonzero, but as we shall explain later, they are.). The full tables for $p < 25000$ may be found on the author's webpage.

p	k	$(e_{1,k}, e_{3,k}, \ldots, e_{p-2,k})$
37	32	(1 26 0 36 1 35 31 34 3 6 2 36 1 0 11 36 11 26)
59	44	(1 45 21 30 14 35 5 0 48 57 7 52 2 11 0 54 24 45 29 38 14 58 27 32 15 0 44 27 32)
67	58	(1 45 38 56 0 47 62 9 29 15 65 26 45 57 0 10 22 41 2 52 38 58 5 20 0 11 29 22 66 2 24 43 65)
101	68	(1 56 40 96 26 63 0 61 81 71 35 92 73 64 6 88 0 0 13 95 37 28 9 66 30 20 40 0 38 75 5 61 45 100 17 17 12 66 72 53 86 31 70 15 48 29 35 89 84 84)
691	12	(1 222 647 44 469 690 177 81 234 351 224 0 78 250 507 149 363 359 177 2 250 451 ...)

The last row is given so one can compare two of its entries with the periods of the normalized weight 12 cuspidal eigenform Δ with Fourier coefficients given by the Ramanunjan τ-function. It might be surprising that $\frac{e_{3,k}}{e_{5,k}}$ and $\frac{r_3(\Delta)}{r_5(\Delta)} = -\frac{14}{9}$ (see Example 3.4.15) are the same modulo 691!

The existence of an essentially unique nontrivial pairing in our computations led us to the following conjecture [**McSh**].

CONJECTURE 5.1.12 (MCCALLUM-S.). *The elements $e_{i,k}$ for odd i and even k generate $A^- \otimes_{\mathbb{Z}} \mu_p$. In other words, the map*

$$\mathcal{C}_1 \otimes_{\mathbb{Z}_p} \mathcal{C}_1 \to A_1^- \otimes_{\mathbb{Z}} \mu_{p^n}$$

induced by the pairing $(\ ,\ )_1$ is surjective.

Let's take a short detour to explain some reasons the values of this pairing are interesting. First, they give the powers appearing in commutators in relations in a presentation of the Galois group $G_{F,S}$ of the maximal pro-p, p-ramified extension of F.

REMARK 5.1.13. Let $\mathcal{G}$ denote the maximal pro-p quotient of $G_{F,S}$. Being a finitely generated pro-p group, it fits in an exact sequence

$$1 \to \mathcal{R} \to \mathcal{F} \to \mathcal{G} \to 1,$$

where $\mathcal{F}$ is a free pro-p group on a minimal finite number d of generators, and $\mathcal{R}$ is a free pro-p subgroup that is generated as a normal subgroup of $\mathcal{F}$ by a minimal finite number r of elements.

Suppose that p is odd and F contains μ_p. As groups, we then have

$$H^i(G_{F,S}, \mu_p^{\otimes i}) \cong H^i(\mathcal{G}, \mathbb{F}_p) \cong \mathrm{Hom}(\mathcal{F}/\mathcal{F}_1, \mathbb{F}_p)$$

for $i \in \{1, 2\}$, where $\mathcal{F}_1 = \mathcal{F}^p[\mathcal{F}, \mathcal{F}]$. Fixing a set of d generators x_i of $\mathcal{G}$, we have a dual basis x_i^* to their images in the maximal elementary abelian p-quotient $\mathcal{F}/\mathcal{F}_1 \cong \mathcal{G}/\mathcal{G}_1$ inside the latter homomorphism group. The cup products $x_i^* \cup x_j^*$ give a collection elements of

$$H^2(\mathcal{G}, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathcal{G}}(\mathcal{R}, \mathbb{F}_p),$$

the latter isomorphism being the inverse of the transgression map in the Hochschild-Serre spectral sequence. This allows us to evaluate $x_i^* \cup x_j^*$ at a relation $r \in \mathcal{R}$. The result $r_{i,j}$ is the power of $[x_i, x_j]$ occuring the expression of the relation $r \in \mathcal{F}_1$ modulo pth powers and triple commutators:

$$r \in \left(\prod_{1 \le i < j \le d} [x_i, x_j]^{r_{i,j}} \right) \mathcal{F}^p[\mathcal{F}, [\mathcal{F}, \mathcal{F}]],$$

where one might note that the ordering of the product does not matter.

For our second application, we want to consider continuous Galois cohomology groups $H^1(G_{K,S}, T)$ with coefficients in a finitely generated module T over a compact local $\mathbb{Z}_p$-algebra R with finite residue field (e.g., $R = \mathbb{Z}_p$). This cohomology, defined via continuous cochains, has the property that

$$H^i(G_{K,S}, T) \cong \varprojlim_n H^i(G_{K,S}, T/\mathfrak{m}^n T)$$

for all $i \ge 0$, where $\mathfrak{m}$ is the maximal ideal of R.

REMARK 5.1.14. Since $G_{K,S}$ has cohomological dimension 2, we always have

$$H^2(G_{K,S}, T/\mathfrak{m}^n T) \cong H^2(G_{K,S}, T) \otimes_R R/\mathfrak{m}^n R.$$

EXAMPLE 5.1.15. Upon taking inverse limits of the exact sequences of Proposition 5.1.5, we obtain a canonical isomorphism

$$H^1(G_{K,S}, \mathbb{Z}_p(1)) \cong \mathcal{E}_{K,S}$$

and a canonical exact sequence

$$0 \to \mathrm{Cl}_{K,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^2(G_{K,S}, \mathbb{Z}_p(1)) \to \bigoplus_{v \in S} \mathbb{Z}_p \xrightarrow{\sum} \mathbb{Z}_p \to 0.$$

REMARK 5.1.16. Since $G_{K,S}$ has cohomological dimension 2, if L/K is any Galois extension with Galois group G and we use S also to denote the primes over S in K, then for any T as above we have an isomorphism

$$H^2(G_{L,S}, T)_G \xrightarrow{\sim} H^2(G_{K,S}, T)$$

from the coinvariant group of $H^2(G_{L,S}, T)$, i.e., the maximal quotient of $H^2(G_{L,S}, T)$ on which G acts trivially. Note that the coinvariant group M_G of an $R[G]$-module M is isomorphic to $M/I_G M$, where I_G is the augmentation ideal in $R[G]$.

It is often remarkably useful to think of cup products as connecting homomorphisms.

LEMMA 5.1.17. *Let L/K be an S-ramified abelian pro-p extension of K with Galois group G. The connecting homomorphism*

$$\Psi_{L/K,S} \colon H^1(G_{K,S}, \mathbb{Z}_p(1)) \to H^2(G_{K,S}, G(1))$$

in the long exact sequence associated to the short-exact sequence

$$0 \to G \xrightarrow{g \mapsto g-1} \mathbb{Z}_p[G]/I_G^2 \xrightarrow{g \mapsto 1} \mathbb{Z}_p \to 0 \tag{5.1.4}$$

satisfies $a \mapsto a \cup \pi_G$, where $\pi_G \colon G_{K,S} \to G$ is the projection map.

DEFINITION 5.1.18. We call the map $\Psi_{L/K,S}$ the S-recriprocity map for L/K. When L is taken to be the maximal abelian pro-p S-ramified extension of K, we write $\Psi_{K,S}$ for $\Psi_{L/K,S}$ and refer to it simply as the S-reciprocity map for K.

Using S-reciprocity maps, we can give the following description of the second graded quotient of $H^2(G_{L,S}, \mathbb{Z}_p(1))$ in its augmentation filtration (cf. [**Sha1**]).

PROPOSITION 5.1.19. *Let L/K be an S-ramified abelian pro-p extension. Then we have a canonical isomorphism*

$$\frac{I_G H^2(G_{L,S}, \mathbb{Z}_p(1))}{I_G^2 H^2(G_{L,S}, \mathbb{Z}_p(1))} \cong \frac{H^2(G_{K,S}, G(1))}{\Psi_{L/K,S}(\mathcal{E}_{K,S})}.$$

In our specific case of interest, we have the following. Let $A_{K,S}$ denote the p-part of the S-class group $\mathrm{Cl}_{K,S}$.

COROLLARY 5.1.20. *Let Φ be a subgroup of $\mathcal{B}_{n,F_n,S}$, and let E_n be the Kummer extension of F_n obtained by adjoining all p^nth roots of elements of Φ. Suppose that E_n/F_n is totally ramified*

at the unique prime over p. Set $G = \mathrm{Gal}(E_n/F_n)$. The norm map induces an isomorphism $(A_{E_n,S})_G \xrightarrow{\sim} A_n$, and we have an isomorphism

$$\frac{I_G A_{E_n,S}}{I_G^2 A_{E_n,S}} \cong \frac{A_n \otimes_{\mathbb{Z}_p} G}{\Psi_{E_n/F_n,S}(\mathcal{E}_n)}$$

These are isomorphisms of $\mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$-modules if $E_n/\mathbb{Q}$ is Galois, i.e., if $\Phi F_n^{\times p^n}$ is preserved by $\mathrm{Gal}(F_n/\mathbb{Q})$.

Note in the above that while $A_{E_n,S}$ does not have a canonical $\mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$-module structure, its graded quotients in the augmentation filtration do.

EXAMPLE 5.1.21. Consider the extension $E = F(\eta_i^{1/p})$ of F for an odd integer i. It has Galois group $G \cong \mu_p^{\otimes i}$ as a $\mathbb{Z}_p[\Delta]$-module. Suppose that Vandiver's conjecture holds at p and that $i \not\equiv \pm(k-1) \bmod p$ for all even integers k with $p \mid B_{1,\omega^{k-1}}$. If $e_{i,k} \neq 0$ for all such k (i.e., if pairing with η_i is surjective), then $A_E \cong A_F$ via the norm map.

This is shown using Corollary 5.1.20. The key point beyond its application is that if $I_G A_E / I_G^2 A_E = 0$, then $A_E \cong (A_E)_G$, and since E/F is ramified at p, the norm map induces an isomorphism $(A_E)_G \cong A_F$. The condition that $i \not\equiv 1-k \bmod p-1$ insures this ramification, and the condition that $i \not\equiv k-1 \bmod p-1$ then insures that $A_{E,S} \cong A_E$.

5.2. Iwasawa cohomology

We maintain the notation of Section 5.1. Note that since K cannot contain all p-power roots of unity, the groups $H^2(G_{K,S}, \mathbb{Z}_p(1))$ and $H^2(G_{K,S}, \mathbb{Z}_p(2))$ need not be isomorphic. In fact, while $H^2(G_{K,S}, \mathbb{Z}_p(2))$ is a finite group, the group $H^2(G_{K,S}, \mathbb{Z}_p(1))$ need not be finite, as Remark (5.1.15) shows. This presents a problem if we wish to consider the application of cup products

$$H^1(G_{K,S}, \mathbb{Z}_p(1)) \times H^1(G_{K,S}, \mathbb{Z}_p(1)) \to H^2(G_{K,S}, \mathbb{Z}_p(2))$$

to the structure of class groups. This can be remedied to an extent by passing up the cyclotomic $\mathbb{Z}_p$-extension under corestriction maps. Recall the notation for cyclotomic $\mathbb{Z}_p$-extensions from Remark 2.3.1.

DEFINITION 5.2.1. Let T be a compact $R[\![G_{K,S}]\!]$-module, where R is a compact $\mathbb{Z}_p$-algebra. For $i \geq 0$, the ith Iwasawa cohomology group of K_∞ with T-coefficients is the $R[\![\Gamma]\!]$-module

$$H^i_{\mathrm{Iw},S}(K_\infty, T) = \varprojlim_n H^i(G_{K_n,S}, T),$$

where the inverse limit is taken with respect to corestriction maps.

EXERCISE 5.2.2. Show that $H^0_{\mathrm{Iw},S}(K_\infty, T) = 0$.

REMARK 5.2.3. For $R = \mathbb{Z}_p$, we have

$$H^2_{\mathrm{Iw},S}(K_\infty, T) \cong \varprojlim_n H^2(G_{K_n,S}, T/p^n T),$$

If $\mu_q \subset K$, then $\mu_{p^r} \subset K_n$, so G_{F_n} acts trivially on μ_{p^n}. We can then pull Tate twists out of the groups: i.e., we have isomorphisms

$$H^2_{\mathrm{Iw},S}(F_\infty, T(i)) \cong H^2_{\mathrm{Iw},S}(F_\infty, T)(i)$$

of $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$-modules for all $i \in \mathbb{Z}$. Each group $H^2(G_{K,S}, T(i))$ is then determined by the group $H^2_{\mathrm{Iw},S}(K_\infty, T)$ as a coinvariant group of the ith Tate twist:

$$H^2(G_{K,S}, T(i)) \cong (H^2_{\mathrm{Iw},S}(K_\infty, T)(i))_\Gamma$$

EXAMPLE 5.2.4. We have in the notation of Section 2.5 that

$$H^1_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(1)) \cong \mathcal{E}_\infty \quad \text{and} \quad H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(1)) \cong X_\infty.$$

In particular, $H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2)) \cong X_\infty(1)$.

If we replace F by any number field, the first isomorphism holds for the inverse limit of p-completions of p-units in the fields K_n, but for the second, one has an exact sequence as in Example 5.1.15.

$$0 \to X'_\infty \to H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \to \bigoplus_{v \in S} \mathbb{Z}_p[\Gamma/\Gamma_v] \to \mathbb{Z}_p \to 0,$$

where X'_∞ denotes the completely split Iwasawa module over K_∞, which is to say the Galois group of the maximal abelian pro-p extension of K_∞ in which all primes (over p) split completely, and Γ_v denotes the decomposition group at v in $\Gamma = \mathrm{Gal}(K_\infty/K)$.

We can define S-reciprocity maps at the level of K_∞. Let $\mathcal{E}_{K_\infty} = \varprojlim_n \mathcal{E}_{K_n,S}$ under norm maps (which is independent of S containing the primes over p).

DEFINITION 5.2.5. Let L_∞ be an S-ramified abelian pro-p extension of K_∞ with Galois group G. The S-reciprocity map

$$\Psi_{L_\infty/K_\infty,S} \colon \mathcal{E}_{K_\infty} \to H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \hat{\otimes}_{\mathbb{Z}_p} G,$$

where $\hat{\otimes}_{\mathbb{Z}_p}$ denotes the completed tensor product (i.e., inverse limit of tensor products of quotients by closed subgroups) is the map induced by the connecting homomorphism

$$H^1_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \to H^2_{\mathrm{Iw},S}(K_\infty, G(1))$$

for the long exact sequence attached to the short exact sequence of (5.1.4). If L_∞ is the maximal S-ramified abelian pro-p extension of K_∞, we write $\Psi_{K_\infty,S}$ for $\Psi_{L_\infty/K_\infty,S}$.

EXERCISE 5.2.6. Determine how this map interpolates (inverse limits of) cup products.

The analogues to Proposition 5.1.19 and Corollary 5.1.20 for Iwasawa cohomology are then as follows.

PROPOSITION 5.2.7. *Let L_∞/K_∞ be an S-ramified abelian pro-p extension with Galois group $G = \mathrm{Gal}(L_\infty/K_\infty)$. Then we have a canonical isomorphism*

$$\frac{I_G H^2_{\mathrm{Iw},S}(L_\infty, \mathbb{Z}_p(1))}{I_G^2 H^2_{\mathrm{Iw},S}(L_\infty, \mathbb{Z}_p(1))} \cong \frac{H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \hat{\otimes}_{\mathbb{Z}_p} G}{\Psi_{L_\infty/K_\infty,S}(\mathcal{E}_{K_\infty})},$$

which is of Λ-modules if L_∞/K is Galois.

Specializing to our specific case of interest that $F = \mathbb{Q}(\mu_p)$ and $S = \{(1-\zeta_p)\}$, we have the following.

COROLLARY 5.2.8. *Suppose that Φ is a closed $\mathrm{Gal}(F_\infty/\mathbb{Q})$-stable subgroup of the p-completion of the p-unit group of F_∞. Let E_∞ be the Kummer extension of F_∞ obtained by adjoining all p-power roots of elements of Φ, which is then Galois over $\mathbb{Q}$, and suppose it is totally ramified at the unique prime over p. Set $G = \mathrm{Gal}(E_\infty/F_\infty)$. Let X'_{E_∞} denote the inverse limit of p-parts of S-class groups of number fields in E_∞. If E_∞ has a unique prime over p, then $(X'_{E_\infty})_G \cong X_\infty$, and we have a canonical isomorphism*

$$\frac{I_G X'_{E_\infty}}{I_G^2 X'_{E_\infty}} \cong \frac{X_\infty \otimes_{\mathbb{Z}_p} G}{\Psi_{E_\infty/K_\infty,S}(\mathcal{E}_\infty)}$$

of $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!]$-modules.

EXAMPLE 5.2.9. We may for instance take E_∞ to be given by adjoining to F_∞ all p-power roots of $\eta_i \in \mathcal{E}_\infty$ for some i as in Example 5.1.21. Note that $\mathrm{Gal}(E_\infty/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ for a particular choice of semi-direct product. In this case, under the assumptions of said example (i.e., pairing with η_i is surjective), we have $X_{E_\infty} \cong X_{F_\infty}$, as can be seen by Nakayama's lemma. In particular, it would appear to be typical behavior that the unramified Iwasawa module X_{E_∞} is finitely generated over $\mathbb{Z}_p$, though in principle it could be much larger! It's reasonable to ask the open question of whether this is always the case.

5.3. K-groups and Steinberg symbols

We can interpret the Galois cohomology groups in question as K-groups of S-integer rings via a standard description of K_1 and a theorem of Tate. We keep the assumptions and notations of the previous two sections. For definitions and properties of the lower (resp., higher) K-groups, see the book of Milnor [**Mil**] (resp., Weibel [**Wei**]).

We have $K_1(\mathcal{O}_{K,S}) \cong \mathcal{O}_{K,S}^\times$, so

$$K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^1(G_{K,S}, \mathbb{Z}_p(1)),$$

and Tate showed the existence of a canonical isomorphism

$$K_2(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^2(G_{K,S}, \mathbb{Z}_p(2)).$$

We have product maps in K-theory, in particular

$$K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} K_1(\mathcal{O}_{K,S}) \to K_2(\mathcal{O}_{K,S}),$$

the image of $a \otimes b$ being what is known as the Steinberg symbol $\{a, b\}$ (see Milnor's book).

PROPOSITION 5.3.1. *We have a commutative diagram*

$$\begin{array}{ccc} K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} K_1(\mathcal{O}_{K,S}) & \xrightarrow{\{\,,\,\}} & K_2(\mathcal{O}_{K,S}) \\ \downarrow & & \downarrow \\ H^1(G_{K,S}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(G_{K,S}, \mathbb{Z}_p(1)) & \xrightarrow{\cup} & H^2(G_{K,S}, \mathbb{Z}_p(2)). \end{array}$$

REMARK 5.3.2. At primes in S, we have tame symbols on $K_2(\mathcal{O}_{K,S})$, which for any $v \in S$ (which we treat as an additive valuation) with residue field k_v, which are given by the composition of $K_2(\mathcal{O}_{K,S}) \to K_2(K)$ with the map

$$K_2(K) \to k_v^\times, \qquad \{a,b\} \mapsto (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}},$$

recalling that $K_2(K)$ is generated by Steinberg symbols by the theorem of Matsumoto. There is a canonical exact sequence

$$0 \to K_2(\mathcal{O}_K) \to K_2(\mathcal{O}_{K,S}) \to \bigoplus_{v \in S} k_v^\times \to 0.$$

Note that $k_v^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0$ if v lies over p.

More generally, the Quillen-Lichtenbaum conjecture, which was proven as a consequence of the work of Voevodsky and Rost, gives us the following isomorphisms.

THEOREM 5.3.3. *For $j \in \{1,2\}$ and any $i \geq 1$, there are canonical isomorphisms*

$$c_{i,j} \colon K_{2i-j}(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} H^j(G_{K,S}, \mathbb{Z}_p(i))$$

compatible with products in K-theory and cup products.

EXAMPLE 5.3.4. Suppose that p is odd. For even $k \geq 2$, the quotient of the p-parts of the orders of $K_{2k-2}(\mathbb{Z})$ and $K_{2k-1}(\mathbb{Z})$ is $p^{v_p(B_k/k)}$. Explicitly, for any $i \geq 1$, we have

$$K_{2i-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^2(G_{\mathbb{Q},S}, \mathbb{Z}_p(i)) \cong (X_\infty^{(1-i)}(i-1))_\Gamma,$$
$$K_{2i-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p(i)) \hookleftarrow (\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma,$$

where the latter injection has cokernel $(X_\infty^{(1-i)}(i-1))^\Gamma$. If i is odd and $X^{(1-i)} = 0$, then $(\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma \cong \mathbb{Z}_p$ is generated by the image of a certain limit of cyclotomic p-units. If i is even, then $(X_\infty^{(1-i)}(i-1))^\Gamma = 0$, and $(\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma$ is isomorphic to the finite group $\mathbb{Z}_p(i-1)_{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})}$. It follows that, under Vanidver's conjecture at p, the nonvanishing of $e_{i,k}$ is equivalent to the surjectivity of the products

$$K_{2i-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} K_{2(k-i)-1}(\mathbb{Z}) \to K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

for odd $i \geq 1$ and even $k \geq 2$.

5.4. The map ϖ

We begin by defining a special class of modular symbols inside the first homology group of a modular curve relative to its cusps. Let N be a positive integer. Recall that $\mathcal{M}_2(N) = H_1(X_1(N), C_1(N), \mathbb{Z})$.

DEFINITION 5.4.1. For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, the Manin symbol $[u:v]_N \in \mathcal{M}_2(N)$ is

$$[u:v]_N = \left\{ \frac{b}{d} \to \frac{a}{c} \right\}_N,$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $u = c \bmod N$ and $v = d \bmod N$.

The reader can check that $[u:v]_N$ exists and is well-defined. Note that $[u:v]_N = \gamma\{0 \to \infty\}_N$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is as in the definition of $[u:v]_N$. Manin proved the follwing [**Man1**].

THEOREM 5.4.2 (MANIN). *The group $\mathcal{M}_2(N)$ is generated by the Manin symbols $[u:v]_N$ with $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, and it is presented by these symbols subject to the relations*

$$[u:v]_N = [-u:-v]_N = -[-v:u]_N = [u:u+v]_N + [u+v:v]_N$$

for all such u and v.

PROOF THAT THE RELATIONS HOLD. The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. Note that $S^2 = T^3 = -I$, and $-I$ fixes all cusps, thus all modular symbols. The latter implies the first equality. Note that

$$\{0 \to \infty\}_N + S\{0 \to \infty\}_N = \{0 \to \infty\}_N + \{\infty \to 0\}_N = 0$$

and

$$\{0 \to \infty\}_N + T\{0 \to \infty\}_N + T^2\{0 \to \infty\}_N = \{0 \to \infty\}_N + \{-1 \to 0\}_N + \{\infty \to -1\}_N = 0.$$

Applying $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to these relations yields the relations on Manin symbols. □

REMARK 5.4.3. There is also a presentation of $\mathcal{M}_k(N)$ in terms of Manin symbols, again having the form

$$X^{i-1}Y^{k-i-1}[u:v] = \gamma \cdot X^{i-1}Y^{k-i-1}\{0 \to \infty\}$$

with $u, v \in \mathbb{Z}/N\mathbb{Z}$ and $(u,v) = (1)$, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $(u,v) = (c,d) \bmod N\mathbb{Z}^2$ (cf. [**Mer**]).

DEFINITION 5.4.4. Set $\mathbb{Z}' = \mathbb{Z}[\frac{1}{2}]$. For a $\mathbb{Z}$-module M with a commuting action of a complex conjugation τ (i.e., an involution) and $m \in M$, we set $M^+ = (M \otimes_{\mathbb{Z}} \mathbb{Z}')^+$ and $m^+ = \frac{1}{2}(m + \tau(m)) \in M^+$.

For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, we have

$$[u:v]_N^+ = \frac{1}{2}([u:v]_N + [-u:v]_N) \in \mathcal{M}_2(N)^+.$$

DEFINITION 5.4.5. For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, we set

$$[u:v]_N^* = w_N[u:v]_N^+ = \left\{\frac{d}{bN} \to \frac{c}{aN}\right\}^+ \in \mathcal{M}_2(N)^+.$$

DEFINITION 5.4.6. The non-zero cusps $C_1^\circ(N)$ of $X_1(N)$ are the cusps that do not lie over the cusp $0 \in X_0(N)$.

The zero cusps in $X_1(N)$, i.e., those that map to $0 \in X_0(N)$, are exactly those represented by a reduced fraction $\frac{a}{c}$ with c prime N. We have the following corollary of Theorem 5.4.2 for the relative homology group

$$\mathcal{S}_2^\circ(N) = H_1(X_1(N), C_1^\circ(N), \mathbb{Z}).$$

COROLLARY 5.4.7. *The group $\mathcal{S}_2^\circ(N)^+$ is generated by the $[u:v]_N^*$ with $u,v \in \mathbb{Z}/N\mathbb{Z} - \{0\}$ and $(u,v) = (1)$, subject to the relations*

$$[u:v]_N^* = [-u:v]_N^* = -[v:u]_N^* = [u:u+v]_N^* + [u+v:v]_N^*$$

for u, v as above (noting that the last term is zero if $u+v=0$).

Let us use a subscript N when denoting Steinberg symbols in $K_2(\mathbb{Z}[\frac{1}{N}, \mu_N])$. The following was proven independently in nearly this form by Busuioc [**Bus**] and the author [**Sha3**].

PROPOSITION 5.4.8 (BUSUIOC, SHARIFI). *There exists a map*

$$\Pi_N^\circ \colon \mathcal{S}_2^\circ(N)^+ \to K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N])^+$$

satisfying

$$\Pi_N^\circ([u:v]_N^*) = \{1-\zeta_N^u, 1-\zeta_N^v\}_N^+$$

for all $u, v \in \mathbb{Z}/N\mathbb{Z} - \{0\}$ with $(u,v) = (1)$.

PROOF. We need only show that Π_N° respects the relations of Corollary 5.4.7. Dirichlet's unit theorem tells us that

$$\mathbb{Z}[\mu_N]^\times \cong \mu_M \oplus (\mathbb{Z}[\mu_N]^+)^\times / \langle -1 \rangle.$$

where $M = N$ or $2N$ depending on whether N is even or odd, respectively. For $\zeta \in \mu_M$, we have $\{\zeta, \zeta\}_N = 0$ by antisymmetry, and we have $\{\zeta, u\}_N^+ = 0$ for all $u \in (\mathbb{Z}[\mu_N]^+)^\times$ as $\{\zeta, u\}_N$ is inverted by complex conjugation. Thus, $\{\zeta, v\}_N^+ = 0$ for all $v \in \mathbb{Z}[\mu_N]^\times$.

Now, note that $1 - \zeta_N^u = -\zeta_N^u(1-\zeta_N^{-u})$, so we have

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = \{1-\zeta_N^{-u}, 1-\zeta_N^v\}_N^+,$$

Moreover, Steinberg symbols are antisymmetric, so in particular we have

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = -\{1-\zeta_N^v, 1-\zeta_N^u\}_N^+.$$

Finally, we note that

$$\frac{1-\zeta_N^u}{1-\zeta_N^{u+v}} + \zeta_N^u \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}} = 1,$$

so

$$\left\{ \frac{1-\zeta_N^u}{1-\zeta_N^{u+v}}, \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}} \right\}_N^+ = 0,$$

which yields

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = \{1-\zeta_N^u, 1-\zeta_N^{u+v}\}_N^+ + \{1-\zeta_N^{u+v}, 1-\zeta_N^v\}_N^+$$

by bilinearity and antisymmetry. □

REMARK 5.4.9. The map Π_N° satisfies $\Pi_N^\circ(\langle j \rangle^{-1} x) = \sigma_j \Pi^\circ(x)$ for all $x \in \mathcal{S}^\circ(2)(N)^+$ and all $j \in (\mathbb{Z}/N\mathbb{Z})^\times$.

The following lemma was proven by Fukaya and Kato on p-completions for p dividing N.

LEMMA 5.4.10. *The map Π_N° restricts to a map*

$$\Pi_N \colon \mathcal{S}_2(N)^+ \to K_2(\mathbb{Z}[\mu_N])^+.$$

PROOF. For a prime ℓ, let q_ℓ denote the order of the residue field of a fixed prime over ℓ in $\mathbb{Q}(\mu_N)$. We claim that there exists a map f as in the diagram

$$\begin{array}{ccc} H_1(X_1(N), C_1^\circ(N), \mathbb{Z}') & \longrightarrow & \mathbb{Z}'[C_1^\circ(N)] \\ \downarrow{\scriptstyle \Pi_N^\circ} & & \downarrow{\scriptstyle f} \\ K_2(\mathbb{Z}[\frac{1}{N}, \mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}' & \longrightarrow & \bigoplus_{\ell | N} \mathbb{F}_{q_\ell}^\times \otimes_{\mathbb{Z}} \mathbb{Z}' \end{array} \tag{5.4.1}$$

that makes it commute, where the upper horizontal arrow is the boundary map, the lower horizontal arrow is the sum of tame symbols (see Remark 5.3.2) at our fixed primes over $\ell \mid N$. (Here, we consider Π_N° to be zero on the minus part of homology.)

We define the projection f_ℓ of the map f to the ℓ-coordinate of the direct sum. For an integer n, let n_ℓ denote the ℓ-part of (n, N), and let $n'_\ell = \frac{n}{n_\ell}$. For a non-zero cusp $\{\frac{c}{aN}\}$, where $\frac{a}{c}$ is in reduced form and a is prime to N, set $f_\ell(\{\frac{c}{aN}\}) = 1$ unless (c, N) is a power of ℓ, and otherwise set

$$f_\ell\left(\left\{\frac{c}{aN}\right\}\right) = \begin{cases} (1 - \zeta_{N'_\ell}^{(aN_\ell)^{-1}})^{-c_\ell} & \text{if } N'_\ell \neq 1 \\ c'_\ell & \text{if } N'_\ell = 1. \end{cases}$$

The commutativity is now left as an exercise. □

Merel provided rather nice formulas for the action of Hecke operators on Manin symbols [**Mer**].

THEOREM 5.4.11 (MEREL). *For a positive integer n and $u, v \in \mathbb{Z}/n\mathbb{Z}$ with $(u, v) = (1)$, we have*

$$T_n([u : v]_N) = \sum_{\substack{a,b,c,d \geq 0 \\ ad-bc=n \\ a>b,\, d>c}} [au + cv : bu + dv]_N,$$

where we take $[x : y]_N$ to be zero if $(x, y) \neq (1)$.

EXAMPLE 5.4.12. We have

$$T_2([u : v]_N) = [2u : v]_N + [2u : u + v]_N + [u + v : 2v]_N + [u : 2v]_N. \tag{5.4.2}$$

and

$$\begin{aligned} T_3([u : v]_N) = {} & [3u : v]_N + [3u : u + v]_N + [3u : 2u + v]_N \\ & + [2u + v : u + 2v]_N + [u + 2v : 3v]_N + [u + v : 3v]_N + [u : 3v]_N. \end{aligned} \tag{5.4.3}$$

The reader might try the fun computation that the relations (5.1.2) and (5.4.2) (resp., (5.1.3) and (5.4.3)) yield the cases $\ell = 2, 3$ in the following theorem of Fukaya and Kato, which was conjectured in a slightly weaker form (that Π_N is Eisenstein in the same sense as what follows) in [**Sha3**, Conjecture 5.8].

THEOREM 5.4.13 (FUKAYA-KATO). *Suppose that $p \mid N$ is an prime greater than 3. For every prime $\ell \geq 1$, the map*

$$\Pi_N^\circ \colon \mathcal{S}_2^\circ(N)^+ \otimes \mathbb{Z}_p \to K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N])^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

satisfies

$$\Pi_N^\circ \circ (T_\ell - 1 - \ell\langle\ell\rangle) = 0$$

for all primes $\ell \nmid N$ *and* $\Pi_N^\circ(U_\ell - 1) = 0$ *for all primes* $\ell \mid N$.

Sketch of proof of Theorem 5.4.13. Via a regulator computation, Fukaya and Kato exhibit the Hecke-equivariance of a map

$$z_N^\sharp \colon \mathcal{S}_2^\circ(N) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^2_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Q}_p(2))^{\text{ord}}$$

that takes a symbol $[u : v]^*$ to a Beilinson-Kato element $g_u \cup g_v$, where g_u and g_v are the Siegel units on $Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}$ of Remark 3.2.9. This map is not in general integral, but the growth of its denominators can be controlled in the tower of increasing p-power levels (and the maps are compatible with degeneracy maps and corestriction), so for the purpose of this sketch, we can suppose it takes values in $H^2_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2))^{\text{ord}}$.

For any $i \geq 0$, there exists a map

$$\infty \colon H^i_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2)) \to H^i(G_{\mathbb{Q}(\mu_N),S}, \mathbb{Z}_p(2)),$$

where S is the set of primes of $\mathbb{Q}(\mu_N)$ over N, associated to pullback by the cusp at infinity, which is not quite a point on $Y_1(N)$ but may be viewed as a morphism

$$\infty \colon \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}, \mu_N]^+(\!(q)\!) \to Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}.$$

The map is pullback followed by a composition

$$H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N](\!(q)\!), \mathbb{Z}_p(2))^+ \to H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N][\![q]\!], \mathbb{Z}_p(2))^+ \xrightarrow{q \mapsto 0} H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N], \mathbb{Z}_p(2))^+,$$

the first map being a splitting of the canonical surjection. We note that the latter étale cohomology group is isomorphic to $H^i(G_{\mathbb{Q}(\mu_N),S_N}, \mathbb{Z}_p(2))^+$ for S_N the set of primes of $\mathbb{Q}(\mu_N)$ over N. These maps are compatible with cup products.

The effect of ∞ on g_u is to forget about the power of q that occurs in its q-expansion and then evaluate it at 0, which results in a root of unity times $1 - \zeta_N^u$. Thus, $\infty \circ z_N^\sharp([u : v]_N) = \{1-\zeta_N^u, 1-\zeta_N^v\}_N$. The result then follows from the Hecke-equivariance of $z^\sharp$ and the computable facts that for any ℓ prime to N, one has $\infty \circ (T_\ell - 1 - \ell\langle\ell\rangle) = 0$, while for all ℓ dividing N, one has $\infty((U_\ell - 1)(g_u \cup g_v)) = 0$, which in particular implies that $z_N^\sharp([u : v]_N)$ and its ordinary projection have the same image under ∞. Thus $\Pi_N^\circ = \infty \circ z^\sharp$, and it is Eisenstein in the sense defined in the theorem. □

In particular, Π_N° and Π_N factor through maps

$$\varpi_N^\circ \colon \mathcal{S}_2^\circ(N)^+/I\mathcal{S}_2^\circ(N)^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to (K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^+$$

and

$$\varpi_N \colon \mathcal{S}_2(N)^+/I\mathcal{S}_2(N)^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to (K_2(\mathbb{Z}[\mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^+.$$

For any prime ℓ dividing N, a Manin-type symbol $[\ell u : v]^*_{N\ell} \in \mathcal{S}_2(N\ell)$ maps to $[u : v]^*_N$ under the degeneracy map ϵ_1 on homology, and $\{1-\zeta_N^u, 1-\zeta_{N\ell}^v\}_{N\ell}$ has norm $\{1-\zeta_N^u, 1-\zeta_N^v\}_N$. That is, the maps $\varpi_{N\ell}$ and ϖ_N are compatible.

5.5. A conjecture and known results

We now return to the Hida-theoretic and Iwasawa-theoretic settings, again restricting to the modular tower $X_1(p^r)$ and the cyclotomic tower $F_r = \mathbb{Q}(\mu_{p^r})$ for a fixed irregular prime p. Let $k \geq 2$ be an even integer such that $p \mid B_{2,\omega^{k-2}}$. We adopt the notation of Section 4.3 and work on the modular side with localizations at the Eisenstein maximal ideal $\mathfrak{m}_k$.

We recall our map Υ and define a map ϖ out of the maps ϖ_{p^r} of the previous section. For S the set consisting of the prime over p in F, let us set

$$Y = H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2))^{(2-k)} \cong X_\infty^{(1-k)}(1),$$

as in Example 5.2.4. The map Υ then becomes a map $\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$.

Using the isomorphisms

$$(K_2(\mathbb{Z}[\mu_{p^r}]) \otimes \mathbb{Z}_p)^+ \xrightarrow{\sim} H^2(\mathbb{Z}[\tfrac{1}{p}, \mu_{p^r}], \mathbb{Z}_p(2))^+$$

that are compatible with norms and corestriction, we may view $\varprojlim_r (\varpi_r \otimes_{\mathbb{Z}} \mathrm{id}_{\mathbb{Z}_p})$ as a map to $X_\infty(1)$ from the inverse limit of the groups $\mathcal{S}_2(p^r)/I\mathcal{S}_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ under the degeneracy maps induced by the identity on $\mathbb{H}$. We define $\varpi\colon \mathcal{S}/I\mathcal{S} \to Y$ to be the resulting map on ω^{2-k}-eigenspaces.

Remark 5.5.1. In our current setting, it makes no difference whether we work with the maps ϖ_{p^r} or $\varpi^\circ_{p^r}$, as

$$(\mathfrak{S}_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\mathrm{ord}} = (\mathfrak{S}^\circ_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\mathrm{ord}}.$$

In fact, repeated application of U_p to a cusp $\left\{\frac{a}{b}\right\}$ with p dividing b yields a formal sum of cusps with increasing power of p in the denominator, until that power reaches p^r, at which point each application multiplies the sum by p. Therefore, any such non-zero cusp must have trivial image in the ordinary part of the $\mathbb{Z}_p$-modular symbols.

The following conjecture can be viewed as a refinement of the main conjecture of Iwasawa theory (cf. [**Sha3**, Conjecture 4.12]).

Conjecture 5.5.2. *The maps $\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$ and $\varpi\colon \mathcal{S}/I\mathcal{S} \to Y$ are inverse to each other.*

Fukaya and Kato have proven strong results towards Conjecture 5.5.2, most importantly [**FuKa**, Theorem 7.2.3(1)]. Let $\xi' \in \Lambda$ be the power series in Λ that satisfies

$$\xi'(\upsilon^s - 1) = (1 - p^{-1})L'_p(\omega^k, s-1)$$

for all $s \in \mathbb{Z}_p$. As a power series in T, it equals $(T+1)\frac{d\xi}{dT}$.

Theorem 5.5.3 (Fukaya-Kato, Fukaya-Kato-S.). *The identity $\xi'\Upsilon \circ \varpi = \xi'$ holds on $\mathcal{S}/I\mathcal{S}$.*

Specifically, Fukaya and Kato proved that $\xi'\Upsilon \circ \varpi = \xi'$ on $\mathcal{S}/I\mathcal{S} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, but it since it was not at that time a priori clear that $\mathcal{S}/I\mathcal{S}$ has no p-torsion, this original result was ostensibly weaker. The result is strengthened to the above statement as a consequence of [**FKS2**]. In a recent preprint [**Oht4**], Ohta proves the following theorem, which shows that $\mathcal{S}/I\mathcal{S}$ indeed has no p-torsion.

THEOREM 5.5.4 (OHTA). *The map Υ is an isomorphism.*

When the tame level is not 1, certain characters are excluded from Ohta's result, but in our situation it has this simple form. Wake and Wang-Erickson had previously proven, using the theory of pseudo-deformations, that Υ is a pseudo-isomorphism under Greenberg's conjecture (without Ohta's condition on the character) and an isomorphism under Vandiver's conjecture [**WWE1, WWE2**]. In fact, what they show is that under Vandiver's conjecture is that the two Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ are Gorenstein, and under Greenberg's conjecture, they are weakly Gorenstein in a specific sense. In [**Sha3**, Proposition 4.10], it had been pointed out that if $\mathfrak{H}$ is Gorenstein, then Υ is an isomorphism.

COROLLARY 5.5.5. *If ξ and ξ' are relatively prime in Λ, then Conjecture 5.5.2 holds.*

PROOF. If ξ and ξ' are relatively prime, then in that (ξ) is its characteristic ideal, the Λ-module Y must be pseudo-cyclic. By the main conjecture and the fact that Y is p-torsion free by Proposition 2.3.21, there then exists an injective pseudo-isomorphism $Y \to \Lambda/(\xi)$. The map $\xi' \colon Y \to Y$ given by multiplication by ξ' is then injective, and since Υ is an isomorphism by Theorem 5.5.4, the map $\xi' \colon \mathcal{S}/I\mathcal{S} \to \mathcal{S}/I\mathcal{S}$ is injective as well. By Theorem 5.5.3, we then have that $\Upsilon \circ \varpi = 1$, so given that Υ is an isomorphism, the maps Υ and ϖ are inverse to each other. □

REMARK 5.5.6. If Greenberg conjecture fails, then ξ and ξ' necessarily have a common factor. If Greenberg's conjecture holds, then Y is pseudo-cyclic as a Λ-module, but it is possible that ξ has a square factor.

REMARK 5.5.7. If $X_\infty^{(1-k)}$ is merely supposed to be pseudo-cyclic, which is a consequence of Greenberg's conjecture, then we may conclude from the above theorems that ϖ is an isomorphism and $\Upsilon \circ \varpi$ and $\varpi \circ \Upsilon$ are multiplication by a unit in Λ that, modulo the annihilator of Y, is independent of all choices. The latter statement is actually the original form of the conjecture in [**Sha3**]: that is, the author strongly suspected at the time that the unit can be taken to be 1 (at least up to sign, with which the careful reader might realize we have been somewhat incautious in this write-up).

REMARK 5.5.8. There are no known cases where ξ and ξ' are not relatively prime, or even in which the λ-invariant of $X_\infty^{(1-k)}$ is greater than 1. (This was checked by Buhler and Harvey for primes $p < 39 \cdot 2^{22}$ in [**BuHa**].) It seems more than likely that ξ never has multiple factors, so Conjecture 5.5.2 in its stated form appears quite reasonable.

Let us very roughly indicate for the interested reader how the two derivatives ξ' appear in the theorem of Fukaya and Kato. On the left, ξ' arises from a rather fascinating computation which says that we have canonical isomorphisms

$$H^i_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \cong Y$$

for both $i = 1$ and $i = 2$, where S is the set consisting of the prime over p in $F = \mathbb{Q}(\mu_p)$. Moreover, the composition

$$Y \xrightarrow{\sim} H^1_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \to H^2_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \xrightarrow{\sim} Y,$$

is ξ', where the second map is cup product with $(1-p^{-1})\log\chi_p \in H^1(G_{\mathbb{Q},S},\mathbb{Z}_p)$. Here, $\log$ denotes the p-adic logarithm defined by the usual power series (which is trivial on roots of unity).

On the right, Fukaya and Kato compute that the composition of a map formed from $z^\sharp$ with a certain p-adic regulator $H^1(G_{\mathbb{Q}_p},\mathcal{T}_{\mathrm{quo}}(1)) \xrightarrow{\sim} \mathfrak{S}$ is, upon reduction modulo I, multiplication by ξ'. (To get to the latter local cohomology group, one must first apply a map in Hochschild-Serre spectral sequence and then restrict.) Here, we use the fact that $\mathcal{S}/I\mathcal{S}$ and $\mathfrak{S}/I\mathfrak{S}$ are canonically isomorphic (given our choice of complex embedding). Though it is rather beyond the scope of these lectures, the point is that

$$L_p'(\omega^k, s-1) = \lim_{t\to 0} \zeta_p(t+1)(L_p(\omega^k, s+t-1) - L_p(\omega^k, s-1)),$$

where ζ_p is the p-adic Riemann-zeta function. The two-variable power series interpolating $\zeta_p(t+1)L_p(\omega^k, s+t-1)$ appears in a p-adic regulator computation on the value $z(\{0\to\infty\})$ of a map $z\colon \mathcal{M} \to H^1_{\mathrm{Iw},S}(F_\infty, \tilde{\mathcal{T}}(1))$ constructed using Beilinson-Kato elements on the curves $Y(p^r)$, and which descends to $(1-U_p)z^\sharp$ under corestriction maps, upon restriction to $\mathcal{S}$. The p-adic regulator of (or Coleman map applied to) $z(\{0\to\infty\})$ is a power series attached to a two-variable p-adic L-function valued in modular forms, and at $t=0$ it is a product of two Λ-adic Eisenstein series (one suitably diagonalized), the constant term of which is the above product of L-functions. The derivative appears in applying the Manin-Drinfeld splitting (which allows us to subtract off $\zeta_p(t+1)L_p(\omega^k, s-1)$) and in letting t tend to zero, which amounts to descending down the cyclotomic tower.

We end by describing an alternate form of Conjecture 5.5.2, which by Corollary 5.2.8 gives an analytic invariant (conjecturally) describing the structure of the second graded quotient in the augmentation filtration of the completely split Iwasawa module over the maximal p-ramified abelian pro-p extension of F_∞.

Definition 5.5.9. We define a map $\phi\colon \mathfrak{X}_\infty^- \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times/\langle -1\rangle]\!](1)$ by

$$\phi(\sigma) = \varprojlim_n \sum_{\substack{i=1\\ p\nmid j}}^{p^r-1} \chi_{i,n}(1-\zeta_{p^n}^i)[i]_n,$$

where $\chi_{i,n}\colon \mathfrak{X}_\infty \to \mu_{p^n}$ denotes the Kummer character attached to a p^nth root of $1-\zeta_{p^r}^i$ and $[i]_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times/\langle -1\rangle$ denotes the group element attached to i. Let $\Phi\colon \mathfrak{X}_\infty^-(-1) \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+$ be its twist by $\mathbb{Z}_p(-1)$.

Remark 5.5.10. The map ϕ has kernel isomorphic to the quotient of the Tate twist of the "Iwasawa adjoint" $\alpha(X_\infty^+)$, which is p-torsion free and pseudo-isomorphic to $(X_\infty^+)^\iota(1)$, and cokernel isomorphic to $(X_\infty^+[p^\infty])^\vee(1)$. In particular, it is an injective pseudo-isomorphism under Greenberg's conjecture at p and an isomorphism under Vandiver's conjecture at p.

Let $1-\zeta = (1-\zeta_{p^r})_r \in \mathcal{E}_\infty$. Let $\Psi_\infty\colon \mathcal{E}_\infty \to X_\infty^{(1-k)} \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^+$ denote the composition of the S-reciprocity map $\Psi_{K_\infty,S}$ with projection to the appropriate eigenspaces.

DEFINITION 5.5.11. We define the universal ordinary Mazur-Tate element (cf. [**MaTa**]) by

$$\mathcal{L} = \varprojlim_n \sum_{\substack{j=0 \\ p\nmid j}}^{p^r-1} U_p^{-r}[j:1]_r^\star \otimes [j]_r \in \mathcal{T}_{\mathfrak{m}}^+ \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+,$$

and we let $\overline{\mathcal{L}}$ denote its image in $\mathcal{S}/I\mathcal{S} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+$.

The universal ordinary Mazur-Tate element gives rise to (as written, the plus part of) the two-variable p-adic L-function of Mazur-Kitagawa by specialization at a Λ-adic (or A-adic for a Λ-algebra A) eigenform [**Kit**].

Note that $X_\infty^{(1-k)} \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^- \cong X_\infty^{(1-k)}(1) \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^-(-1)$, so it makes sense to apply $\Upsilon \otimes \Phi$ to the former tensor product. We arrive at the following alternate form of Conjecture 5.5.2.

CONJECTURE 5.5.12. *We have* $(\Upsilon \otimes \Phi) \circ \Psi_\infty(1-\zeta) = \overline{\mathcal{L}}$.

APPENDIX A

Project descriptions

A.1. First project

Let N be a integer prime to an odd prime p. We consider the prime-to-p part Δ' of the group $\Delta = (\mathbb{Z}/Np\mathbb{Z})^\times/\langle -1\rangle$. Let $\theta\colon \Delta' \to \overline{\mathbb{Q}}_p^\times$ be a character. We consider $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ as a compact $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-module by allowing a group element j to acts as $\langle j\rangle^{-1}$. Let $F = \mathbb{Q}(\mu_{Np})$ and F_∞ be its cyclotomic $\mathbb{Z}_p$-extension, and note that $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_{p,N}^\times$. Set

$$Y = H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2))_\theta,$$

where S is the set of primes of F over p.

For a $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-module M, we may consider its θ-eigenspace for the group Δ':

$$M_\theta = M \otimes_{\mathbb{Z}_p[\Delta']} \mathcal{O}_\theta,$$

where $\mathcal{O}_\theta$ is the $\mathbb{Z}_p$-algebra generated by the image of θ. This is (noncanonically) a direct summand of M, and it is an $\mathcal{O}_\theta[\![T]\!]$-module.

Consider the Hecke algebra $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ for $\Lambda = \mathbb{Z}_p[\![T]\!]$, and define an Eisenstein ideal I to be generated by the images of $T_\ell - 1 - \ell\langle\ell\rangle$ for $\ell \nmid Np$ and $U_\ell - 1$ for $\ell \mid Np$. There is a unique maximal ideal $\mathfrak{m}$ of $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ containing I. We still have the group

$$\mathcal{T} = \varprojlim_r H^1_{\text{ét}}(X_1(Np^r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))_{\mathfrak{m}},$$

which fits in an $\mathcal{O}_\theta[\![G_{\mathbb{Q}_p}]\!]$-exact sequence as in (4.3.2) with $D(\mathcal{T}_{\mathrm{quo}}) \cong \mathfrak{S} = S(N,\Lambda)_{\mathfrak{m}}$ and its Λ-dual $\mathcal{T}_{\mathrm{sub}}$ free of rank 1 over $\mathfrak{h} = \mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_{\mathfrak{m}}$.

In **[Sha3]**, it is shown that if $p \geq 5$, $p \nmid \varphi(N)$, and the character θ is primitive, satisfies $\theta\omega^{-1}(p) \neq 1$ when considered as primitive Dirichlet character, then we can as before construct out of $\mathcal{T}$ a Λ-module homomorphism

$$\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$$

that is conjectured to be an isomorphism, inverse to $\varpi = \varprojlim_r (\varpi_{Np^r})_\theta$. (Here, we consider the p-part of ϖ_{Np^r} as it was defined before, and we view it as a map to $H^2(G_{F_r,S}, \mathbb{Z}_p(2))^+$.) The conditions we placed on θ were sufficient to insure that the canonical map $X_\infty(1)_\theta \to Y$ is an isomorphism, where X_∞ is the unramified Iwasawa module.

The project:

(1) Remove the condition $p \nmid \varphi(N)$ from the construction of Υ.
(2) Construct Υ for as wide a class of θ as possible: note that $\mathcal{T}$ may not quite be the right object for this! It should be helpful to think of Υ as a connecting homomorphism **[Sha4]**.
(3) Formulate the analogous conjecture to Conjecture 5.5.2 in the θ-eigenspace.

A.2. Second project

Let K be an imaginary quadratic field, and fix $N \geq 4$. We consider the ray class field $K(N)$ of K. Let (E, P) be the canonical CM pair of modulus N over $K(N)$ in the sense of [**Kat**, (15.3.1)]. In particular, E has CM by $\mathcal{O}_K$ and $E(\mathbb{C}) \cong \mathbb{C}/N\mathcal{O}_K$ under an isomorphism taking P to 1. For a nontrivial integral ideal $\mathfrak{c}$ of $\mathcal{O}_F$ prime to $6N$, we have a θ-function ${}_{\mathfrak{c}}\theta_E$. (If $\mathfrak{c} = (c)$ for some $c > 1$, then this is simply the pullback from the universal elliptic curve of the θ-function ${}_c\theta$ of Definition 3.2.6.) For a nonzero $u \in \mathbb{Z}/N\mathbb{Z}$, we obtain an elliptic N-unit ${}_{\mathfrak{c}}\Theta_N(u) = {}_{\mathfrak{c}}\theta_E(uP)^{-1} \in \mathcal{O}_{K(N)}[\frac{1}{N}]^\times$, which is in fact a unit unless $N\mathcal{O}_K$ is a prime power. For the Galois element $\sigma_{\mathfrak{c}} \in G_K^{\mathrm{ab}}$ corresponding to $\mathfrak{c}$ by class field theory, the element

$$\Theta_N(u) = {}_{\mathfrak{c}}\Theta_N(u) \otimes (N(\mathfrak{c}) - \sigma_{\mathfrak{c}})^{-1} \in \mathcal{O}_{K(N)}[\tfrac{1}{N}]^\times \otimes_{\mathbb{Z}} \mathcal{Q},$$

where $\mathcal{Q}$ is the total quotient ring of $\mathbb{Z}_p[\mathrm{Gal}(K(N)/K)]$, is independent of $\mathfrak{c}$. If one ignores this issue of integrality, one could ask if there exists a well-defined map

$$\Pi_N^\circ \colon H_1(X_1(N), C_1^\circ(N), \mathbb{Z}_p) \to K_2(\mathcal{O}_{K(N)}[\tfrac{1}{N}]) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \qquad [u : v]_N^\star \mapsto \{\Theta_N(u), \Theta_N(v)\}_N,$$

where we use a slightly different notation for symbols here by not projecting to "plus parts". Note that the K_2-group is finite, which creates an apparent issue given the denominators used in the definition of the $\Theta_N(u)$.

The project:

(1) Show that Π_N° is a well-defined map under assumptions on the level or to certain eigenspaces for the action of Galois. (Here, it may be best to look at elliptic units arising as specializations of Siegel units on $Y_1(N)$, assuming the Heegner hypothesis on N.)
(2) Determine whether the restriction of Π_N° to $H_1(X_1(N), \mathbb{Z}_p)$ takes image in cohomology of $G_{K(N),S_p}$, for S_p the set of primes over p.
(3) Show that Π_N arises as specialization of the map $z_N^\sharp$ of Fukaya-Kato at the CM point (E, P). Determine whether this specialization factors through the quotient of homology by a certain CM ideal I_N, producing a map ϖ_N.
(4) Can there be an equivariance of ϖ_N for diamond operators and Galois elements, and if so, what is it? Determine whether or not this map should be expected to be surjective (or injective).
(5) What difference does the ramification behavior of p in K make? Perform computations in examples.

The methods of [**FKS2**] could be helpful in the first part. The passage to an inverse limit over increasing p-power in the levels, as in [**FuKa**], could also be helpful in avoiding issues of torsion. For the last part, we note that a more natural map might arise by replacing the homology of $X_1(N)$ with the (first relative) homology of the Bianchi space of level N, which for Euclidean fields has nice Manin-type generators and relations, with the generator indexed by pairs of relatively prime elements of $\mathcal{O}_F/N$, as proven by Cremona [**Cre**]. (This could also be investigated.) In comparison, the map above only uses a limited set of pairs of elliptic N-units.

A.3. Third project

This project has as its goal the exploration of the relationship between Massey products of units of cyclotomic fields and the Iwasawa theory of Kummer extensions (see [**Sha2**]). There are numerous possibilities here. First, let us recall the definition of Massey products.

For a profinite group G and a commutative ring R, a defining system for an n-fold Massey product $(\chi_1, \dots, \chi_n)$ of n continuous homomorphisms $\chi_i \colon G \to R$ is a homomorphism $\rho \colon G \to N_{n+1}/Z_{n+1}$, where N_{n+1} denotes the group of upper-triangular unipotent matrices in $\mathrm{GL}_{n+1}(R)$ and Z_{n+1} denotes the subgroup of matrices which are zero above the diagonal aside from the $(1, n+1)$-entry, such that the character $\rho_{i,i+1}$ given by the $(i, i+1)$-entry of ρ is χ_i for $1 \leq i \leq n$. Given such a defining system, the Massey product $(\chi_1, \dots, \chi_n)$ is taken to be the class of the 2-cocycle

$$\kappa_{1,n}(\sigma, \tau) \mapsto \sum_{i=2}^{n} \rho_{1,i}(\sigma)\rho_{n+2-i,n+1}(\tau).$$

The Massey product is therefore only defined if there exists such a defining system, and if so, its value depends upon the choice of defining system. Thus, it may be viewed as an element of a quotient of $H^2(G, R)$. Note that we may also extend the definition to R-coefficients upon which G acts by a character to $R^\times$ by placing products of the characters along the diagonal and requiring that the resulting map to the upper-triangular Borel be a homomorphism.

Now, let us focus for the moment on Massey triple products (a_1, a_2, a_3) of elements of $\mathcal{E}_{F,S}$ for a number field F containing μ_p and S a set of primes containing those dividing p. (We omit subscripts for simplicity of notation.) Taken with $\mathbb{Z}_p(1)$-coefficients, such a Massey product will exist if and only if $(a_1, a_2) = (a_2, a_3) = 0$, in which case it will have image in the quotient of $H^2(G_{F,S}, \mathbb{Z}_p(3))$ by all cup products of the form (a_1, c) and (c, a_3) where $c \in H^1(G_{F,S}, \mathbb{Z}_p(2))$.

The project:

(1) By definition, the Massey product (a_1, a_2, a_3) provides an obstruction to the existence of a certain p-ramified extension. Under what circumstance does the vanishing of such products correspond to the existence of a (different) unramified extension of a p-extension of F in the sense of Corollary 5.1.20 (for $F = \mathbb{Q}(\mu_p)$)? What about higher Massey products? Study the implications for the structure of unramified Iwasawa modules.

(2) Consider Massey products of the form $(\chi_p, \dots, \chi_p, a_1, \dots, a_n)$ as elements of quotients of $H^2(G_{F,S}, \mathbb{Z}_p(n))$, where $\chi_p \in H^1(G_{F,S}, \mathbb{Z}_p)$ is the cyclotomic character. What are these measuring? (For $n = 1$, one might compare with [**McSh**, Section 4] for $F = \mathbb{Q}(\mu_p)$ and μ_p-coefficients.)

(3) In Iwasawa theory (taking $F = \mathbb{Q}(\mu_p)$), we have a duality between $\mathfrak{X}_\infty^+$ and X_∞^- (see, e.g., (2.3.18)). Do we have related duality for the second graded quotient of an unramified Iwasawa module of a Kummer extension that is controlled by cup products with a Kummer generator? What about for higher Massey products? The paper [**LiSh**] might be a good reference for duality.

For an extra fun challenge, see if n-fold Massey products of cyclotomic units can be interpreted in terms of some variant of modular symbols for GL_n. (This can be discussed if we come to it.)

A.4. Fourth project

The goal of this project is to formulate a higher weight version of Conjecture 5.5.2 at level one (or tame level), relating Steinberg symbols of Soulé (or cyclotomic) elements in higher K-groups and higher weight modular symbols. Set $\mathbb{Z}' = \mathbb{Z}[\frac{1}{2}]$, as before.

The project:

(1) For even $k \geq 2$, construct a map

$$\Pi_k \colon \mathcal{S}_k(1, \mathbb{Z}') \to K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}'$$

the projection of which to $K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ takes $X^{i-1}Y^{k-i-1}\{0 \to \infty\}$ for $3 \leq i \leq k-3$ and odd i to a Steinberg symbol $\{\kappa_i, \kappa_{k-i}\}$ of elements $\kappa_j \in K_{2j-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for odd j that are constructed out of cyclotomic p-units, known as Soulé elements [**Sou**].

(2) Determine whether an alternate construction of Π_k can be made without reference to individual primes.

(3) Show that Π_k factors through the quotient of $\mathcal{S}_k(1, \mathbb{Z}')$ by an Eisenstein ideal I_k generated by $T_\ell - 1 - \ell^{k-1}$ for all primes ℓ, inducing a map ϖ_k.

(4) Construct a map $\Upsilon_k \colon K_{2k-2}(\mathbb{Z}) \otimes \mathbb{Z}' \to \mathcal{S}_k(1, \mathbb{Z}')/I_k\mathcal{S}_k(1, \mathbb{Z}')$ out of the Galois action on the higher weight p-adic étale cohomology groups of a modular curve.

(5) Show that $\xi_k' \Upsilon_k \circ \varpi_k = \xi_k'$ for a particular number ξ_k'.

(6) Compare the above with the Λ-adic weight 2 constructions in the notes.

(7) Repeat the previous steps allowing an arbitrary tame level N.

Bibliography

[BuHa] J. P. Buhler, D. Harvey, Irregular primes up to 163 million, *Math. Comp.* **80** (2011), 2435–2444.

[Bus] C. Busuioc, The Steinberg symbol and special values of L-functions, *Trans. Amer. Math. Soc.* **360** (2008), 5999–6015.

[CoLi] J. Coates, S. Lichtenbaum, On ℓ-adic zeta functions, *Ann. of Math* **98** (1973), 498–550.

[Col1] R. Coleman, Division values in local fields, *Invent. Math.* **53** (1979), 91–116.

[Col2] R. Coleman, Local units modulo cyclotomic units, *Proc. Amer. Math. Soc.* **89** (1983), 1–7.

[Con] B. Conrad, Arithmetic moduli of generalized elliptic curves, *J. Inst. Math. Jussieu* **6** (2007), 209–278.

[Cre] J. Cremona, Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields, *Compos. Math.* **51** (1984), 275–324.

[Del] P. Deligne, Formes modulaires et représentations l-adiques, *Séminaire Bourbaki*, Exp. 355, *Lecture Notes in Math.* **175**, Springer, Berlin, 1971, 139–172.

[DeRa] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), *Lecture Notes in Math.* **349**, Springer, Berlin, 1973, 143–316.

[DiSh] F. Diamond, J. Shurman, A first course in modular forms, *Grad. Texts in Math.* **228**, Springer, New York, 2005.

[Dri] V. Drinfeld, Two theorems on modular curves, *Funkcional. Anal. i Priložen* **7** (1973), 83–84.

[Eme] M. Emerton, The Eisenstein ideal in Hida's ordinary Hecke algebra. *Int. Math. Res. Not. IMRN* **1999** (1999), 793–802.

[FeGr] B. Ferrero, R. Greenberg, On the behavior of p-adic L-functions at s=0. *Invent. Math.* **50** (1978/79), 91–102.

[FeWa] B. Ferrero, L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.

[FuKa] T. Fukaya, K. Kato, On conjectures of Sharifi, preprint, version August 15, 2012.

[FKS1] T. Fukaya, K. Kato, R. Sharifi, Modular symbols in Iwasawa theory, In: Iwasawa Theory 2012 - State of the Art and Recent Advances, *Contrib. Math. Comput. Sci.* **7**, Springer, 2014, 177–219.

[FKS2] T. Fukaya, K. Kato, R. Sharifi, Modular symbols and the integrality of zeta elements, *Ann. Math. Qué.* **40** (2016), 377–395.

[Gre1] R. Greenberg, On p-adic L-functions and cyclotomic fields, *Nagoya Math. J.* **56** (1974), 61–77.

[Gre2] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.

[HaPi] G. Harder, R. Pink, Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbf{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen, *Math. Nachr.* **159** (1992), 83–99.

[Hid1] H. Hida, On congruence divisors of cusp forms as factors of the special values of their zeta functions, *Invent. Math.* **64** (1981), 221–262.

[Hid2] H. Hida, Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup.* **19** (1986), 231–273.

[Hid3] H. Hida, Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[\![X]\!])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986), 545–613.

[Hid4] H. Hida, Elementary theory of L-functions and Eisenstein series, London Math. Soc. Stud. Texts **26**, Cambridge Univ. Press, Cambridge, 1993.

[Her] J. Herbrand, Sur les classes des corps circulaires, *J. Math. Pures Appl.* (9) **11** (1932), 417–441.

[Iwa1] K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.

[Iwa2] K. Iwasawa, On the theory of cyclotomic fields, *Ann. of Math.* **70** (1959), 530–561.

[Iwa3] K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964), 42–82.

[Iwa4] K. Iwasawa, Analogies between number fields and function fields, Some Recent Advances in the Basic Sciences, Vol. 2 (Proc. Annual Sci. Conf., Belfer Grad. School Sci., Yeshiva Univ., New York, 1965-1966), Belfer Graduate School of Science, Yeshiva Univ., New York, 203–208.

[Iwa5] K. Iwasawa, On p-adic L-functions, *Ann. of Math.* **89** (1969), 198–205.

[Kat] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, In: Cohomologies p-adiques et applications arithmétiques, III, *Astérisque* **295** (2004), 117–290.

[KaMa] N. Katz, B. Mazur, Arithmetic moduli of elliptic curves. *Ann. of Math. Stud.* **108**, Princeton Univ. Press, Princeton, NJ, 1985.

[Kit] K. Kitagawa, On standard p-adic L-functions of families of elliptic cusp forms, In: p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), *Contemp. Math.* **65**, Amer. Math. Soc., Providence, RI, 1994, 81–110.

[KuLe] T. Kubota, H. Leopoldt, Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.* **214/215** (1964), 328–339.

[Kur] M. Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1. *J. Number Theory* **45** (1993), 281–294.

[Lan] S. Lang, Introduction to modular forms, Grundlehren math. Wiss. **222**, Springer, Berlin-New York, 1976.

[Leo] H. Leopoldt, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, *J. Reine Angew. Math.* **199** (1958), 165–174.

[LiSh] M. Lim, R. Sharifi, Nekovář duality in p-adic Lie extensions of global fields, *Doc. Math.* **18** (2013), 621–678.

[Man1] Y. Manin, Parabolic points and zeta functions of modular curves, *Izv. Ross. Akad. Nauk Ser. Mat.* **36** (1972), 19–66.

[Man2] Y. Manin, Periods of cusp forms, and p-adic Hecke series. *Mat. Sb.* **92(134)** (1973), 378–401, 503.

[MaTa] B. Mazur, J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* **54** (1987), 711–750.

[MaWi1] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.

[MaWi2] B. Mazur, A. Wiles, On p-adic analytic families of Galois representations, *Compos. Math.* **59** (1986), 231–264.

[McSh] W. McCallum, R. Sharifi, A cup product in the Galois cohomology of number fields. *Duke Math. J.* **120** (2003), 269–310.

[Mer] L. Merel, Universal Fourier expansions of modular forms, *On Artin's conjecture for odd 2-dimensional representations*, *Lecture Notes in Math.* **1585**, Springer, Berlin, 1994, 59–94.

[Mil] J. Milnor, Introduction to algebraic K-theory, *Ann. of Math. Stud.* **72**, Princeton Univ. Press, Princeton, NJ, 1971.

[NSW] J. Neurkirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Second Edition, *Grundlehren Math. Wiss.* **323**, Springer-Verlag, Berlin, 2008.

[Oht1] M. Ohta, On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms, *J. reine angew. Math.* **463** (1995), 49–98.

[Oht2] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II, *Math. Ann.* **318** (2000), 557–583.

[Oht3] M. Ohta, Congruence modules related to Eisenstein series, *Ann. Éc. Norm. Sup.* **36** (2003), 225–269.

[Oht4] M. Ohta, μ-type subgroups of $J_1(N)$ and application to cyclotomic fields, preprint, 84 pages.

[Rib] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[Rub] K. Rubin, Appendix to: S. Lang, Cyclotomic fields I and II, Combined second edition, *Grad. Texts in Math.* **121**, Springer-Verlag, New York, 1990, 397–419.

[Ser] J-P. Serre, Classes des corps cyclotomiques (d'après K. Iwasawa), *Séminaire Bourbaki*, Exp. 174, Soc. Math. France, Paris, 1959, 83–93.

[Sha1] R. Sharifi, Massey products and ideal class groups, *J. Reine Angew. Math.* **603** (2007), 1–33.

[Sha2] R. Sharifi, Iwasawa theory and the Eisenstein ideal, *Duke Math. J.* **137** (2007), 63–101.

[Sha3] R. Sharifi, A reciprocity map and the two variable p-adic L-function, *Ann. of Math.* **173** (2011), 251–300.

[Sha4] R. Sharifi, Reciprocity maps with restricted ramification, preprint, arXiv:1609.03616.

[Sha5] R. Sharifi, Iwasawa theory, unpublished lecture notes, http://math.ucla.edu/∼sharifi/iwasawa.pdf.

[Shi1] G. Shimura, Sur les intégrales attachées aux formes automorphes, *J. Math. Soc. Japan* **11** (1959), 291–311.

[Shi2] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Princeton Univ. Press, Princeton, NJ, 1994.

[Sho1] V. Shokurov, A study of the homology of Kuga varieties, *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 443–464, 480.

[Sho2] V. Shokurov, Shimura integrals of cusp forms, *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 670–718, 720.

[Sou] C. Soulé, On higher p-adic regulators, Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), *Lecture Notes in Math.* **854**, Springer, Berlin-New York, 1981, 372–401.

[Sti] L. Stickelberger, Uber eine Verallgemeinerung der Kreistheilung, *Math. Ann.* **37** (1890), 321–367.

[Tat] J. Tate, Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257–274.

[Til] J. Tilouine, Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke, *Bull. Soc. Math. France* **115** (1987), 329–360.

[Was] L. Washington, Introduction to cyclotomic fields, 2nd Ed. *Grad. Texts in Math.* **83**, Springer, New York, 1997.

[Wak] P. Wake, Eisenstein Hecke algebras and conjectures in Iwasawa theory, *Algebra Number Theory* **9** (2015), 53–75.

[WWE1] P. Wake, C. Wang-Erickson, Pseudo-modularity and Iwasawa theory, to appear in *Amer. J. Math.* arXiv:1505.05128.

[WWE2] P. Wake, C. Wang-Erickson, Ordinary pseudorepresentations and modular forms, to appear in *Proc. Amer. Math. Soc.*, arXiv:1510.01661.

[Wei] C. Weibel, The K-book. An introduction to algebraic K-theory, *Grad. Stud. Math.* **145**, Amer. Math. Soc., Providence, RI, 2013.

[Wil1] A. Wiles, On ordinary λ-adic representations associated to modular forms, *Invent. Math.* **94** (1988), 529–573.

[Wil2] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540.